CAPÍTULO 9

LA IDENTIDAD VIRTUAL FRENTE A LOS RIESGOS DE LA SOCIEDAD DIGITAL

Amaryllis Quirós-Ramírez

En los últimos diez años, el acelerado desarrollo de las tecnologías y de la Internet como fenómeno de la globalización, así como el acceso y uso a diversas redes sociales ha conducido a nuevas formas de comunicación y a esquemas de comportamiento interactivo diarios en donde predomina la instantaneidad; las interacciones en el mundo virtual son simultáneas y paralelas, tanto como diversas, cambiantes y amplias, en el sentido de que el espectro de posibles contactos y relaciones de intercambio se puede dar con cualquier persona alrededor del mundo. No existe, en la Sociedad de la Información y el Conocimiento (SIC) contemporánea, un límite geográfico posible, y cada vez se diluyen más las barreras para el acceso y uso generalizado.

Lo anterior se revela no solo en las dinámicas relacionales, como también en la actividad que tienen las redes sociales y la Internet en la sociedad contemporánea. Esto permite afirmar, que el crecimiento de las Tecnologías de la Información y Comunicación (TIC) simboliza el espíritu de la época que vivimos hoy. La tecnología es parte predominante de la vida diaria y responde a múltiples necesidades tanto sociales como individuales; la Internet, como fenómeno social globalizante, cumple un lugar y un papel preponderantes para el desarrollo de múltiples actividades, tanto recreativas y asociadas al entretenimiento, como vinculadas con el aprendizaje y el desarrollo de nuevos conocimientos, con la comunicación interpersonal y masiva en personas de todos los grupos etarios.

Asimismo, la preeminencia del dispositivo móvil en las sociedades contemporáneas es muy alta; de tal manera, se calcula que para el año 2020, existirán alrededor de 36.000 millones de dispositivos móviles inteligentes a nivel mundial (CISCO, 2016). Adicionalmente, estamos conectados a la Internet desde diversos dispositivos de forma cotidiana y constante, a múltiples aplicaciones, a diferentes redes sociales y a múltiples páginas web de forma simultánea.

Nos encontramos, por lo tanto, en una Nueva Sociedad de la Comunicación, en la cual la humanidad se digitalizó, la Internet nos sobrepasa y las tecnologías han tomado todos los espacios de la vida cotidiana de las personas.

Hay un valor innegable relacionado con el desarrollo de esta nueva sociedad tecnológica e interconectada; sin embargo, también se revelan otras consecuencias asociadas con el uso de la diversidad de plataformas web y de aplicaciones a las que los individuos acceden diariamente. Al respecto, se debe considerar que su acceso y uso conllevan -necesariamente- quedar registrado y, por lo tanto, generarse una nueva identidad o varias nuevas otras identidades, las cuales son virtuales. Esto quiere decir que las personas tenemos actualmente múltiples huellas virtuales y que, por lo tanto, exista todo un mundo de sistemas e interconexiones que relacionen la identidad personal con las virtuales. Lo anterior tiene una implicación en términos del manejo de los datos en el ciberespacio y las esferas del mismo en donde se encuentre presente la persona identificada con una *e-Identity* (en diversos sistemas: bancarios, de instituciones de la salud y educativas, por citar tan solo algunos).

Al existir todas estas formas nuevas de registro de la identidad personal-virtual, se potencia entonces, la probabilidad de que los individuos se vean expuestos a riesgos y amenazas informáticos. El mayor acceso a Internet, la proliferación de dispositivos móviles inteligentes, la permanente hiper-conectividad, la posibilidad de automatización, el desarrollo de Internet de las Cosas y la Inteligencia Artificial son algunos de los medios actuales que aumentan el riesgo de eventuales amenazas y de ataques cibernéticos al navegar y existir en el ciberespacio, frente a los cuales, tanto individuos como empresas/corporaciones, instituciones e incluso, Estados y países, quedan expuestos.

Se calcula que para el año 2020, existirán alrededor de 36.000 millones de dispositivos móviles inteligentes a nivel mundial

Los diferentes registros de la identidad virtual potencian la probabilidad de que los individuos se vean expuestos a riesgos y amenazas informáticos

Para el tratamiento de esta temática, este capítulo se estructura siguiendo siete grandes apartados.

El primero de ellos se refiere al tratamiento teórico de algunos conceptos fundamentales sobre el estudio de la identidad en entornos virtuales; posteriormente, el segundo apartado establece una contextualización acerca de los riesgos y amenazas en los entornos virtuales; la tercera parte hace referencia a la nueva sociedad de la comunicación digital; en ella se establece un marco referencial actualizado sobre los usos de los dispositivos tecnológicos y las plataformas digitales. Se plantean aquí valoraciones relacionadas con sus beneficios, pero también consideraciones sobre los posibles perjuicios que conllevan en tanto que amenazas a la identidad virtual. El cuarto eje temático desarrollado establece una tipología de los diferentes riesgos y amenazas prevalecientes en la nueva sociedad de la comunicación digital. La quinta sección del documento establece un marco analítico particular sobre los riesgos y las amenazas a la identidad en las poblaciones menores de edad en Costa Rica. Seguido a ello, el sexto apartado del capítulo se dirige al estudio de elementos relacionados con los delitos informáticos en Costa Rica y el marco legal asociado, desde el entendimiento del marco jurídico relacionado a nivel internacional. Finalmente, en la sétima parte se establecen algunas consideraciones finales sobre la temática general del capítulo, las cuales se plantean como análisis final y con un interés propositivo.

9.1 ANTECEDENTES TEÓRICOS Y CONCEPTUALES

En el curso de este capítulo, será recurrente la referencia al constructo de *identidad personal*, por ello, enseguida se presente un breve marco teórico explicativo de este concepto en su correspondencia con la *comunicación de la identidad virtual*. De igual forma, se exponen elementos relevantes para comprender las relaciones ampliadas entre los conceptos *riesgo, amenaza y seguridad* entendidos dentro del contexto del mundo virtual.

El estudio de la identidad personal tiene una larga historia de desarrollo desde la trayectoria de múltiples disciplinas; las elaboraciones al respecto se dan en la psicología, en las ciencias jurídicas, en la psico-patología y la psiquiatría, en la antropología cultural, en la sociología, en la comunicación y en la literatura, para mencionar solamente algunas de ellas. Varias tradiciones de investigación, sumamente importantes, como es el caso de la Teoría del Desarrollo Psicosocial de Erik H. Eriksson (1950, 2009) dejaron claro que la identidad personal debe, necesariamente de investigarse en su vinculación con las circunstancias históricas; por su parte, George H. Mead (1934, 1968), señaló con muchísima claridad el carácter simbólico y la necesidad de interpretar el Yo, el Sí-mismo y el espíritu de los tiempos (*Zeitgheist*), cuando se estudia la identidad de los sujetos. Empero, no fue sino hasta cuando Erving Goffman (1959, 2001), uno de los teóricos del Interaccionismo Simbólico, introdujo la noción de *autopresentación en la vida cotidiana,* que se comienza a operativizar el concepto de identidad personal para facilitar su investigación. Aunado a lo anterior, la psicología académica contribuyó enormemente cuando estableció las distinciones respectivas y separó los conceptos de identidad, autoestima y autoconcepto.

Desde la antropología y la sociología, la evaluación la identidad de los sujetos se ha ubicado dentro del contexto de la identidad de los pueblos; esto ha llevado primordialmente a las nociones de endogrupo y exogrupo, y, en el plano de los individuos, a las diferencias entre Yo, Nosotros, Ellos, El Otro y Los Otros (Pettigrew, 1998; Turner y Reynolds, 2003; Canto Ortiz y Moral Toranzo, 2005).

En el ámbito de las ciencias jurídicas, sobre todo después de las Revolución Francesa, la identidad se asoció, irremediablemente, con la idea del individuo-ciudadano, *civitas*, con la individualidad y la responsabilidad social. En todos los sistemas societales, el individuo tiene una identidad dentro de un sistema legal que define sus derechos, sus deberes, y sus límites; lo anterior, por supuesto, desde la perspectiva de la normativización de los actos, es decir, del poder (Foucault, 2002), para lo cual, y esto es sumamente importante de mantener presente en este trabajo, el sistema del Gobierno se arroga el derecho de la vigilancia y mantenimiento del registro o huella documental de quién es cada uno de los miembros de su sociedad.

La identidad de las personas hace referencia a las respuestas que, el individuo mismo, quienes le rodean, las instituciones dentro de las cuales interactúa, y los grupos a los que éste pertenece, dan respuesta a la eterna pregunta: *¿Quién soy?* Así, la identidad de una persona contempla no solo lo que piensa sobre sí misma, sino también lo que siente, se imagina y desea sobre sí misma, pero también integra lo que los Otros, las Instituciones y los grupos le atribuyen. Por consiguiente, la

identidad no implica solamente un acontecimiento en tiempo real, sino que integra un fenómeno histórico retrospectivo de su huella, dado por la historia personal y social, y por su proyección prospectiva.

Por otra parte, en la sociedad de la comunicación digital, todos los individuos tienen una identidad -como la señalada en los párrafos anteriores-, pero se le agrega, desde hace aproximadamente un par de décadas, una nueva dimensión, inédita hasta ahora. Hoy por hoy, todos los sujetos tienen su huella virtual en múltiples cuentas y registros, así como una presentación en la Nube Virtual (*Cloud*); de igual manera, en la actualidad, se hace posible tener estimaciones sobre el individuo y sus actos o comportamientos en el mundo (*Big Data*) o segmentaciones de sus perfiles de gustos, de *habitus*. Todo esto es en suma, la referencia a una identidad virtual.

Lo anterior ha conllevado a que, para la mayoría de las personas sea ya usual y cotidiano el acceso y uso regularizado de diversos sitios web de preferencia, así como tener cuentas personales para acceder a las redes sociales, a productos asociados al entretenimiento o la diversión o para realizar transacciones comerciales y financieras, como también para efectos de registro en las instituciones del Estado. Todos estos usos implican que las personas ingresen un perfil de sí mismas, y sus datos personales. De esta manera, ya sea por medio del ingreso directo y personal de datos que hace cada individuo, como a través de la incorporación de datos provenientes de los registros y huellas institucionales, o mediante la alimentación de perfiles generados a partir de algoritmos sobre datos personales, institucionales, laborales o médicos, a todas las personas se nos ha venido creando una identidad en el mundo virtual.

Tal y como se plantea, la identidad personal-virtual tiene múltiples implementaciones, principalmente, para el uso en las interacciones y auto-presentaciones a la hora de establecer comunicación con otras personas, como también cuando se realizan transacciones comerciales y financieras, o incluso para fines presentativos cuando se busca un empleo (*LinkedIn*). Otras formas de uso se dan para el entretenimiento (como en los juegos de roles); de igual manera, para citar algunos otros usos posibles, se da la utilización para instruirse (*Coursera, Youtube*), para acceder a información, socializarla o compartir, pensamientos, opiniones, gustos y preferencias (*Facebook, Instagram, Pinterest*), y hasta para buscar pareja (*Tinder*), entre otros.

Indudablemente, la identidad personal-virtual en la sociedad de la comunicación también presenta especificidades dependiendo de condiciones asociadas al grupo etáreo, al socioeconómico, o a características de grupos socio-políticos de pertenencia; así como a aspectos socio-geográficos, y los referidos a la identidad étnica y de género. De igual manera, al estudiar la identidad personal-virtual, se deben considerar aspectos y condiciones particulares de los individuos pertenecientes a cada grupo, lo cual implica que no se pueda hacer de la misma manera para grupos vulnerables, que para menores de edad, o para personas adultas mayores; como tampoco se haría del mismo modo para expertos y letrados en el ámbito de las nuevas tecnologías que para personas analfabetas de las nuevas tecnologías, o para usuarios frecuentes y usuarios no frecuentes.

Las consideraciones anteriores son justamente relevantes y pertinentes en la medida de que todos estos usos mencionados se convierten en espacios potenciales de riesgos y amenazas.

El entendimiento sobre los riesgos y amenazas posibles a la identidad personal-virtual conlleva establecer la distinción entre lo que define al individuo y lo Otro que es potencial amenaza. La identidad, ya sea de un individuo, de un grupo o de un pueblo es, básicamente, un asunto de límites y de poder, es decir, de control.

La mayoría de las personas aspira poder determinar qué se considera o integra al definirse como individuos y anhelan que sean ellas mismas quienes establezcan los límites al respecto; no obstante, es bien reconocido que esto no es posible y que es necesario hacer transacciones o negociaciones con personas, grupos e instituciones, es decir, hay límites. Con el afán de auto-definirse, los sujetos prefieren exaltar los elementos positivos sobre los negativos y buscan que no se use en contra de sí mismos aquello que ellos mismos han generado. Por lo tanto, la identidad debe ser entonces cuidada o resguardada desde la perspectiva de sus límites y su determinación, esto es, designando lo que cabe dentro de ella y lo que se define fuera de ella, además, del poder que tenga el individuo, las instituciones y/o los otros para definirla. Cuando una persona, una entidad o un grupo aporta elementos que van en detrimento de la determinación de esta definición, o bien, se encuentra en circunstancias y/o situaciones que crean un desbalance desafortunado de las potencialidades jurídicas y normativas de dicha determinación, es cuando se alude al *riesgo*. Es decir, el riesgo refiere a algo que no ha sucedido, pero que potencialmente puede suceder y anticipa una posible amenaza.

El riesgo es algo que existe y que potencia la probabilidad de una amenaza. La amenaza es una situación real asociada a una vulnerabilidad. En el mundo virtual, es la posibilidad latente de que algo pueda ocurrirle a un individuo como usuario de la red

Por su parte, la *amenaza* remite a una situación real -no potencial- que se está dando y que presiona para provocar esa pérdida de determinación de los límites de la identidad que se mencionó; siempre está relacionada con la vulnerabilidad (Lemaître, 2012). El concepto relacionado con la amenaza se refiere a alguien o algo que tiene la capacidad de abusar de la vulnerabilidad de un bien o de una persona. Desde la perspectiva del mundo virtual, refiere propiamente a la posibilidad latente de que algo pueda ocurrirle a un individuo como usuario de la red, por lo que está relacionado con la posible exposición que las personas tienen como cibernautas a riesgos que dañen o lesionen su seguridad e integridad individuales.

La consecuencia de los riesgos y de las amenazas es el aumento de la probabilidad que las personas sean sometidas a situaciones de daño personal, social o institucional. En este sentido, una consecuencia explícita puede ser un perjuicio emocional o físico, una pérdida financiera, o de oportunidades, o bien, un menoscabo al prestigio; el riesgo es, al final de cuentas, una exposición a algo indeseado.

Las personas, los grupos y las instituciones presentan diferentes grados o niveles de vulnerabilidad a los riesgos y las amenazas; también tienen diferencias en las oportunidades de protegerse frente a ellos. Algunas de las formas de protección deben ser implementadas por los individuos, otras por las instituciones y los grupos, y algunas otras por las entidades legales y gubernamentales; inclusive hay otras que son implementadas a nivel de las naciones. La disminución del riesgo y la neutralización de las amenazas integran el concepto de seguridad, y, dentro del mundo virtual, esto refiere a la ciberseguridad (Figura 9.1).

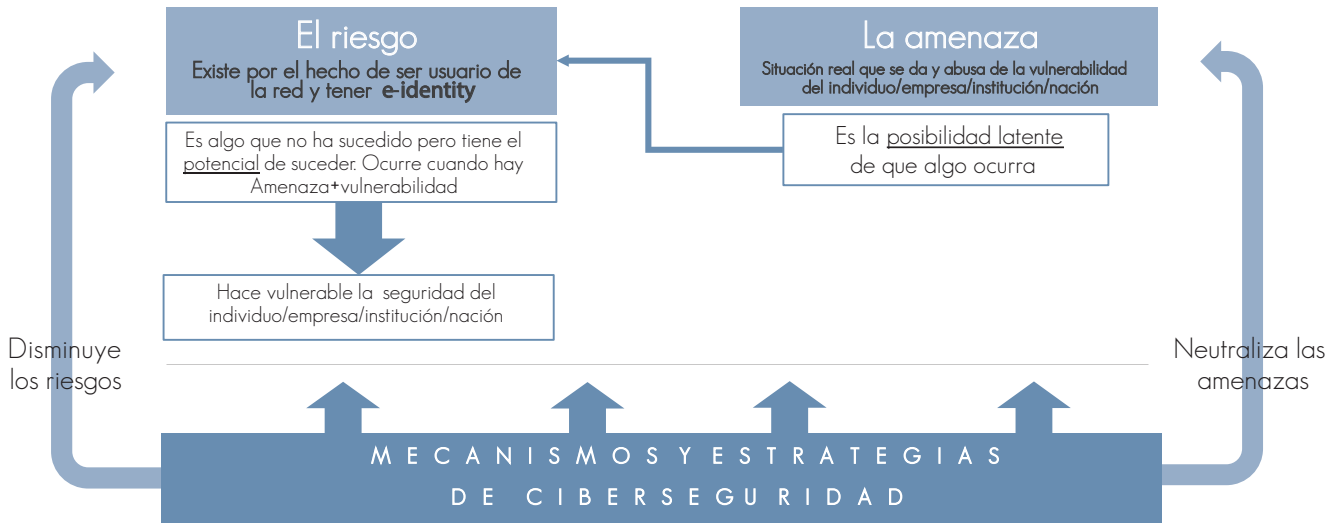

Figura 9.1 Los riesgos y las amenazas a la identidad virtual

Fuente: Elaboración propia.

9.2 CONTEXTUALIZACIÓN SOBRE LOS RIESGOS Y AMENAZAS EN EL MUNDO VIRTUAL

Los fenómenos relacionados con los riesgos, las amenazas y los delitos contra la identidad personal-virtual no son exclusivos del Siglo XXI. La primera situación conocida se registra en 1958 en los Estados Unidos de Norteamérica y, sucesivamente, se han dado otros casos, principalmente en la década de los años ochenta, cuando se registra la primera condena de personas debido a un delito informático en 1983. Esto se da por haber tenido acceso no autorizado a los sistemas de entidades financieras de los Estados Unidos, aunque no existían en ese momento leyes específicas para este tipo de delito[1].

1 Ver: http://www.nytimes.com/1984/03/17/us/two-who-raided-computers-pleading-guilty.html

Posteriormente, la historia registra diversos casos de delitos informáticos, principalmente, por fraude, creación y propagación de códigos maliciosos para afectar cuentas de correos electrónicos, por robo de información financiera y de datos de usuarios; también por sabotaje, por creación de virus contra *hardware* y *software.* Históricamente, se han considerado 8 casos como los más importantes: Richard Stallman (entre 1982 y 1983), David L. Smith de Aberdeen (Crea el *Virus Melissa U* en 1999), Robert Tappan Morris (crea el *Gusano Morris* en 1988), Timothy Lloyd (en 1996), Kevin Poulsen ("Dark Dante", en 1990), Vladimir Levin (en 1995), Gary McKinnon ("Solo", conocido por haber realizado el mayor asalto informático al sistema militar en Estados Unidos y la NASA, en 1997), Kevin Mitnick ("Fantasma de los Cables", en 1981, 1983, 1987 y 1995).

Las amenazas que actualmente se registran con más frecuencia son las estafas o fraudes, tanto a instituciones, o empresas, como a individuos

Con un impacto en el contexto económico-empresarial mundial, trascendió un caso de fraude informático considerado como el más importante en la historia. Este se registró en los Estados Unidos de América y correspondió al robo, entre los años 2005 y 2012, de 160 millones de dólares en Tarjetas de Crédito y Débito de grandes Corporaciones como *NASDAQ, VISA, Dow Jones, Banca Dexia, Carrefour, 7-Eleven*, *Euronet*, *Diners*, entre otras. El delito consistió en instalar un *Malware* en sus bases de datos para robarlas y luego venderlas al mejor postor; llegaban a cobrar $10 por cada número de tarjeta de crédito estadounidense, $50 por cada una que era europea, y $15 por cada una de las canadienses.

Por otra parte, desde un nivel de amenaza y posible afectación a individuos e instituciones o empresas, hoy por hoy lo que parece registrarse con más frecuencia son las estafas o fraudes; se indica que esto se ha favorecido por el contexto en que se da el intercambio de información, es decir por las posibilidades que permite el mundo virtual.

El uso más regularizado de la información digital abre nuevas puertas a requerir datos personales o vinculados con la identidad y la digitalización ha creado nuevos objetivos que han promovido nuevas formas de cometer delitos. Esto se ha visto fomentado tanto por la digitalización de procesos como por la globalización de servicios dados en la web, pues, actualmente, la mayoría de las transacciones (ya sean comunicativas, comerciales, de información, de acceso a servicios, entre múltiples posibilidades) requieren de datos electrónicos y de sistemas automatizados, los cuales permanecen en bases de datos y facilitan a ciber-delincuentes acceder e intervenir en los diferentes ámbitos de la vida cotidiana de las personas; la tecnología informática y las redes sociales contienen información que se pone a disposición y que le permiten al delincuente tener más fácil acceso a información y datos de carácter personal.

Uno de los elementos trasgresores a la identidad, por excelencia (y el más antiguo) ha sido la piratería informática o *Hacking,* el cual ha adquirido dimensiones importantes por el impacto en los objetivos que busca alcanzar: La NASA (*National Aeronautics and Space Administration*), la Fuerza Área de los Estados Unidos, el Pentágono, *Yahoo*, *Google*, *eBay* y el Gobierno de Alemania (Oficina de Naciones Unidas Contra las Drogas y el Delito [UNODC], 2013).

En este sentido, es innegable la existencia latente de la amenaza y la presencia de nuevos ciberataques da cuenta de la prevalencia del riesgo en la sociedad actual. De forma reciente, en marzo de 2018, se registró el caso de ciberataques constantes por parte de *hackers* rusos, denominados "Snake" o conocidos también como "Turla" para obtener información relevante de la red informática del Departamento de Seguridad del Gobierno alemán. La trascendencia del caso se exalta adicionalmente por la frecuencia e intensidad de los ataques, los cuales duraron varios meses y no se expusieron a los medios hasta que se lograra controlarlos.

El caso del delito informático más reciente data de marzo del 2018. Corresponde a una serie de ciberataques por parte de hackers rusos al Departamento de Seguridad del Gobierno alemán

Las actividades relacionadas con los delitos informáticos abarcan un amplio espectro de ámbitos como la provisión de bienes y servicios ilegales; la producción y tráfico de drogas o armas; el tráfico de niños, de órganos o de inmigrantes ilegales; la prostitución; los asesinatos a sueldo; la comercialización de bienes obtenidos por robo o fraude (por ejemplo, automóviles de lujo, obras de arte, animales); la vulneración de normativas medio-ambientalistas, o las inversiones inmobiliarias para lavado de dinero, para mencionar algunas. Todos estos son propiamente delitos vinculados con el crimen organizado y con organizaciones de la Mafia italiana, japonesa, china o rusa. Dentro de estos delitos se encuentran también otros tipos relacionados con la clonación de tarjetas y el robo o hurto de la identidad (criminalidad informática).

De forma generalizada, se ha indicado que el nacimiento y desarrollo de la criminalidad informática está asociada con el desarrollo tecnológico e informático a nivel mundial, siendo ya un fenómeno igualmente transnacional y globalizado, cuyos instrumentos primordiales son los *Crackers*, las computadoras y el Internet para cometer robos, espionajes, sabotajes y extorsiones con fines muchas veces económicos, pero también, de otro tipo. De acuerdo con Acurio del Pino (s.f), aunque muchas veces, el delito informático es de tipo económico, también se vincula con el terrorismo y el ciber-terrorismo, según el nivel de organización y control. En este sentido, puede afectar negativamente tanto a individuos, como a organizaciones institucionales o empresariales, a gobiernos o Estados y a naciones. Esto conlleva cuestionamientos en términos de la capacidad de dar respuesta al fenómeno, en tanto al ser una situación con implicaciones globales, es difícil de controlar.

En seguimiento al marco referencial anteriormente expuesto, este capítulo pretende presentar un panorama descriptivo y analítico documental sobre el desarrollo de las TIC, y particularmente, una aproximación al entendimiento de las interacciones comunicativas mediadas *(On-line Social Networking)* como posibles riesgos y amenazas para la seguridad de la identidad personal, indagando en las situaciones que afectan actualmente a la población digital costarricense en las diferentes actividades y esferas de la vida cotidiana en donde las TIC tienen lugar. Se plantea que, si bien el uso y acceso a las diversas formas y posibilidades que da la Internet conlleva múltiples beneficios, también se ha extendido una contraparte negativa relacionada en donde los riesgos potenciales existen y se encuentran amenazas regulares, constantes y vigentes a la seguridad individual. A esta situación se encuentran expuestas todas las personas, no solo por ingresar a la web y navegar en ella, sino por ser parte conformante en tanto que usuarios con una clave o contraseña, con un perfil creado y con una huella (o múltiples) e identidades virtuales. En este sentido, se considera que el uso de las TIC, de las redes sociales y el acceso a los sitios de interacción en la web tienen una posible incidencia en la identidad personal por las confrontaciones con la seguridad de la identidad virtual.

Por lo anteriormente mencionado, para la escritura de este capítulo, se ha considerado necesario no solo registrar y crear una tipología de las situaciones que son riesgos y amenazas en Costa Rica, como también estudiar el marco legal que se ha ido creando conforme estas situaciones han evolucionado y se han tipificado como *delitos informáticos* en el país.

Se trata, por lo tanto, de identificar las posibles incidencias y repercusiones del *Ser Cibernauta*, considerando que esto puede darse en diferentes momentos del ciclo vital e indistintamente de condiciones o variables socioeconómicas, o de aspectos relacionados con la brecha digital. Adicionalmente, tal y como se ha mencionado, aunque la temática del Internet y sus relaciones con la ciberseguridad atañe hoy mundialmente también a aspectos vinculantes con la seguridad de las naciones y estados (seguridad cívico-política) y los países: ciber-guerras y ciber-terrorismo (Rodríguez, 2016), este análisis se centrará particularmente en las amenazas relativas a la seguridad informática individual. Por lo tanto, se dedicará a estudiar aquellas consecuencias que tienen que ver con el uso de las tecnologías digitales, las redes sociales y los sitios web en las personas usuarias. Desde esta perspectiva, se entenderán entonces las afectaciones negativas a la identidad personal individual y a la seguridad personal. En este caso, se hace referencia al lugar que facilitan las redes sociales y los sitios web como sitios de intercambio que pueden eventualmente conducir a situaciones de abuso, extorsión, *bullying*, dados a través de la web (*ciberbullying*), por mencionar algunas de las situaciones que se presentan actualmente, a personas de diferentes edades en Costa Rica, pero primordialmente a niños, niñas y adolescentes.

9.3 LA NUEVA SOCIEDAD DE LA COMUNICACIÓN Y EL MUNDO DIGITAL

Los últimos 25 años han implicado cambios importantes en el desarrollo tecnológico digital, iniciados a partir de 1990 y principalmente relacionados con las computadoras digitales, la telefonía móvil y el acceso a Internet.

Desde 1982, año en que nace Internet, y, posteriormente en 1991, cuando se formaliza el acceso a la *World Wide Web (*WWW), el crecimiento del acceso de los usuarios a Internet ha sido vertiginoso. Así, durante la primera década del 2000 se desarrolla la presencia masiva de los teléfonos móviles, con tecnología cada vez más avanzada, y del año 2002 al año 2010, la cantidad de usuarios de Internet a nivel mundial casi se ha triplicado, pasando de 631 millones de usuarios (11% de la población mundial) a 1.800 millones (26,6% de la población mundial).

Ese acelerado crecimiento conlleva que, para finales de la primera década del 2000, se diera un uso más generalizado de los dispositivos móviles, con interconectividad de redes móviles; 3.000 millones de personas usaban teléfonos celulares, y

la interconectividad de sitios web y las redes sociales empezaban, en este momento, a ser un estándar en la comunicación digital. Por otro lado, a inicios de la década del 2010, se inicia el acceso a *La Nube* y para el 2015, las *tabletas* y los teléfonos inteligentes son los dispositivos de mayor uso para ingresar a Internet.

De acuerdo con el Reporte *Digital in 2018. Essential Insights into Internet, Social Media, Mobile and E-Commerce Use Around The World* (Hootsuite, 2018), para el mes de enero de este año, el número de usuarios de Internet en el mundo supera la mitad de la población mundial, siendo de 4.000 millones de usuarios, quienes en promedio acceden aseis horas al día; el nivel de penetración de Internet para la región de América Central es de 61%, y el de Social Media es de 59%, el de conectividad móvil de 96% (Figura 9.2).

De lo anterior se desprende que, efectivamente, *Lo Digital* es parte de la vida diaria y que la conectividad se encuentra presente en todos los aspectos de esta cotidianidad, como se ha mencionado (jugar, chatear, buscar productos y servicios, usar servicios públicos o privados, monitorear la salud, hacer deporte, entre muchos otros).

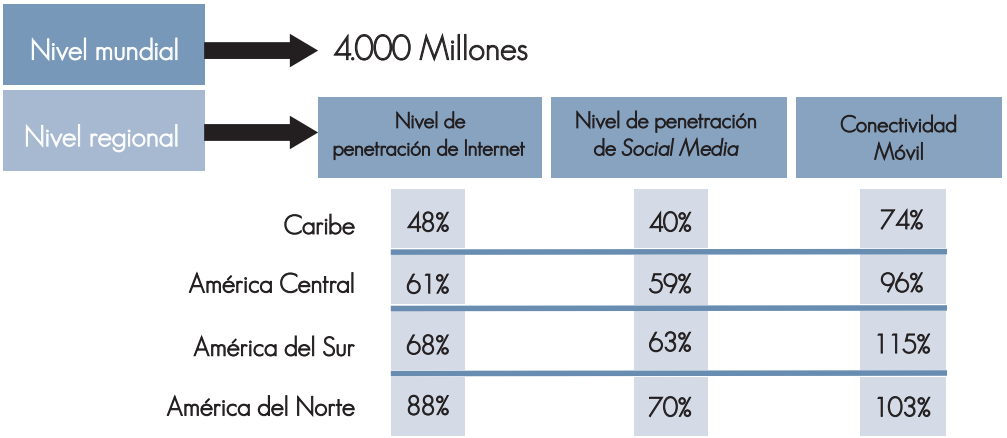

Figura 9.2 Datos sobre penetración de Internet, ***social media*** y conectividad móvil a nivel mundial y para la región

Fuente: Elaboración propia a partir de Hootsuite, 2018.

En cuanto a los usuarios y su vinculación con las redes sociales más importantes, los registros, tanto nacionales como internacionales, indican que *Facebook* sigue siendo la red social más relevante (Hootsuite, 2018; Pew Research Center, 2016; Pantic, 2014), con más de dos mil millones de miembros activos a nivel mundial (Figura 9.3). Al respecto, el registro, para el caso de Costa Rica indica un total de 2.600.000 usuarios para mayo del año 2016 (Latamclick, 2016).

Figura 9.3 Cantidad de usuarios activos en plataformas sociales a nivel mundial (al 27 de enero del 2018)

Fuente: Elaboración propia a partir de Hootsuite, 2018.

De forma más precisa, en la región centroamericana y República Dominicana, el Observatorio de Audiencias Digitales, Ilifebelt (2016), en su estudio anual indica que *Facebook* y *WhatsApp* son las redes de preferencia de los internautas, correspondiendo a 91,2% y 86,6%, respectivamente. Le sigue en cuanto a preferencias para la región, *Google* con 50,8%, *Twitter* con 40,9%, *LinkedIn* con 25,7% y *Snapchat* con 22,9%. Para diciembre del 2017, de acuerdo con *Google Play Store*, *WhatsApp* es la aplicación más importante en Centroamérica y Sur América (Hootsuite, 2018).

Para el caso específico de Costa Rica (Hootsuite, 2018), se registra un nivel de penetración de Internet del 87% (4.29 millones de personas), siendo 3,40 millones de personas los usuarios activos de los medios sociales o *social media* y 3,20 millones los usuarios activos de redes sociales móviles (Figura 9.4).

Figura 9.4 Usuarios activos de Internet, social media y redes sociales móviles en Costa Rica (enero del 2018)

Fuente: Elaboración propia a partir de Hootsuite, 2018.

El estudio Ilifebelt (2016) indica, además, que el uso de las redes sociales sufre cada vez más fragmentación y que integra cada vez más a los usuarios conocidos como *Millenials*; así, los jóvenes de 21 a 30 años representan el 35,5% y los de 31 a 40 años, el 20%; las personas de 51 años o más solamente representan un 7,9%.

Estos datos rectifican la pertinencia de estudiar las relaciones entre la identidad, el sí mismo y la comunicación en mundos virtuales desde su amplitud y multi-dimensionalidad.

Más allá de los aspectos sociales, en la conformación de la identidad se integran variables individuales como el *self* virtual, indicando que los usuarios crean identidades virtuales específicas, pero a la vez proyectan sus fantasías y aspiraciones de su sí mismo a la identidad digital, los cuales se relacionan e impactan entre sí (Nagy y Koles, 2014). Otros autores como Papacharissi (2002), retomando aspectos teóricos de Erving Goffman acerca de la presentación del *self* en la vida cotidiana (*The presentation of self in everyday life*), aportan una perspectiva acerca del impacto positivo de la web en las personas, al indicar que ofrece la expresión de una identidad individual, en tanto es punto de encuentro entre la persona y los miembros de su familia o amigos, siendo un complemento a la interacción *offline*. Papacharissi argumenta cómo en la vida diaria se mantiene un "inter-juego" entre lo que se da o emite y lo que se recibe, y que el individuo mantiene un *performance* en su interior. Plantea que la tecnología se usa para auto-presentarse (por ejemplo, a través del desarrollo de páginas web personales), y que permite rectificar la relación existente entre la identidad personal y la proyección de una identidad virtual (en este caso al destacar cómo se identifican las características personales del *self* a través de un portal o de una página web). De forma específica, distingue, por ejemplo, que en una proyección de un diseño personal, como el de una página web se reflejan marcadores importantes relacionados con el estatus y que los aspectos asociados a los gustos y preferencias o *hobbies* se resaltan mediante hipervínculos para expresar la presentación de la personalidad; se anota que esta forma de manifestarse parece ser equivalente a un ritual social; la tipografía, el color, el uso del espacio, el lenguaje, el tono de la comunicación, se consideran formas de transportar aspectos de la personalidad a la página. Por otro lado, se expresa que los autores de las páginas web también buscan mostrarse mediante elementos como el libro de visitas a la página, y que también buscan afinidad y pertenencia al expresar la afiliación a comunidades de páginas web. Se indica que estos elementos de diseño se usan para mantener un *performance online* a través del cual se manifiesta la personalidad del individuo.

A lo anterior se añaden otras perspectivas enfocadas en el análisis de los entornos virtuales como espacios de presentación personal. En este sentido, Arcila (2010, 2011) estudia los aspectos de la identidad que los individuos buscan proyectar y comunicar al (los) Otro (s), y se interesa en comprender la identidad como objeto de referencia dentro del esfuerzo comunicativo en la interacción mediada. Para ello, estudia la relación Yo-Otros a partir de *chats*, redes sociales y *blogs*, aportando la integración del concepto sí-mismo en el esfuerzo comunicativo que realizan las personas en las interacciones dentro de entornos virtuales. Su hipótesis sostiene que, en la presentación de la identidad en el esfuerzo comunicativo, la producción discursiva se encuentra influenciada por la representación social (o conocimiento previo) que se tiene del Otro: la producción identitaria es mayor cuando existe este conocimiento previo y en las interacciones donde hay un mayor número de contactos virtuales.

En sus investigaciones, el autor busca identificar desde un estudio cuasi-experimental (*pretest-postest*) y mediante el análisis de contenido de redes sociales como *Facebook*, de *chats* y *blogs*, los elementos que se comunican al hablar sobre sí-mismo con otros y su relación con el esfuerzo comunicativo en jóvenes de 18 a 30 años, a partir de una presentación personal en diferentes entornos virtuales de comunicación. El objetivo general es conocer cómo se comunica la identidad y cómo se presentan las personas (auto-presentación del sí-mismo) en entornos virtuales. La hipótesis fundamental indica que la identidad se constituye como objeto de referencia en los procesos de comunicación de los entornos virtuales, siendo relevantes los siguientes aspectos resultantes:

- Los individuos tienden a hablar más de sí mismos conforme buscan nuevos amigos o mantener los contactos que ya tienen (primacía a la representación del otro: cuanto más *alter ego,* se comunica más sobre la identidad).
- Los individuos que hablan más de sí (o muestran su identidad) en *chats* lo hacen con respecto a gustos y preferencias, aspectos que se consideran "conceptos débiles" sobre la identidad.
- En los *blogs*, las categorías identitarias para auto-presentarse son las respuestas evasivas, vagas, genéricas, o anecdóticas y los gustos.
- Hay más propensión a narrar sobre uno mismo conforme hay más socialización virtual (más cantidad de amigos en *Facebook*).
- No se tiende a falsear datos de forma regular, pero se mantienen máscaras importantes sobre aspectos que se consideran fuertemente asociados a la identidad personal como la edad, el nombre, el lugar de residencia, el género, la estatura, la religión.
- Los sujetos tienden a dedicar un esfuerzo comunicativo y apelan a múltiples identidades para hablar de ellos mismos; la mayor parte de la auto-presentación se hace *ad hoc,* haciendo emerger máscaras para situaciones determinadas.

Finalmente, se concluye que el concepto de identidad en la sociedad contemporánea mediada tecnológicamente por la comunicación digital es más difuso y menos concreto en la transmisión del sí mismo. Portillo (2016) añade a lo anterior que existe un distanciamiento cada vez mayor entre la identidad física y el discurso que se emite y tematiza cotidianamente a través de las redes sociales (particularmente, *Facebook, Twitter, Instagram y WhatsApp*), considerando que este distanciamiento es una especie de sustitución de la identidad física por la identidad virtual, en tanto plantea los ciber-discursos como configuradores de identidad.

Todo lo anterior conlleva visualizar un mundo social más amplio, pero también más complejo, y una sociedad del conocimiento que integra más actores y mayores situaciones de atención. Está claro que el desarrollo de las TIC y principalmente la Internet ha traído consigo múltiples beneficios para la SIC, pero también ha tenido como consecuencia que emerjan cambios importantes en las formas en que las personas se comunican e interactúan (Pantic, 2014); también ha implicado que se construyan esquemas diferentes en el esfuerzo comunicativo interpersonal (Arcila, 2010, 2011) que alteran las formas de vinculación personal en relación con el privilegio y uso del dispositivo móvil y todo lo que permite al estar conectado a Internet.

Al respecto, se ha destacado, desde un enfoque centrado en la salud mental, algunos efectos negativos de las redes sociales en los individuos tales como: falsa sensación de conexión, la reducción de la productividad, la pérdida de privacidad, y, cada vez más frecuente, el *ciberbullying (Celada, 2014)*. También se encuentran estudios sobre la relación

Internet ha traído múltiples beneficios a la humanidad, pero también cambios importantes en las formas de comunicación interpersonal. Se han señalado también, ciertos efectos negativos en la salud mental de los individuos

entre el *Online Social Networking o Social Networking Sites* (SNS) y el desarrollo de síntomas depresivos, vinculaciones con la autoestima y la identidad personal (Pantic, 2014). Además, una inquietud cada vez más amplia y generalizada se ha referido al cuestionamiento de qué tan adictivo puede ser el uso de los dispositivos móviles y de las redes sociales, o la necesidad de estar siempre conectados, aunque, al respecto, no ha habido criterios ni datos determinantes.

En el Reino Unido, la *Royal Society for Public Health* (RSPH) y el *Young Health Movement* (YHM) realizaron una encuesta en el año 2017, denominada *#StatusOfMind* (*Social Media and Young People'*s Mental Health), a una muestra de 1500 jóvenes de 14 a 24 años de edad, esto con el fin de medir el impacto de las redes sociales en la salud y el bienestar, en aspectos tales como la ansiedad, la depresión y la imagen corporal.

El primer dato llamativo indicó que el 91% de la población usa Internet para navegar en las redes sociales; además, se expresa que la ansiedad y la depresión han aumentado un 70% en los últimos 25 años y que 7 de cada 10 personas han sido víctimas de *ciberbullying* en algún momento. Adicionalmente, el estudio arroja información sobre las 5 redes sociales más importantes (*Facebook, Instagram, Snapchat, Twitter y Youtube*), indicando que solo esta última causaba un efecto positivo en la salud mental de los adolescentes. Se señala que *Instagram* tiende a ser la red social que causa mayores problemas psicológicos, principalmente asociados a sentimientos de soledad, depresión y ansiedad; y que, en general la conexión constante a las redes sociales altera la calidad del sueño por las notificaciones constantes y estar atento a los mensajes, así como por el contacto con la pantalla (debido a la posible interferencia de la luz LED azul en los mecanismos cerebrales que afectan la producción de la cantidad necesaria para tener un sueño de calidad). De igual forma, se destaca como impacto negativo que las redes generan el fenómeno de "miedo a estarse perdiendo de algo" (*Fear of Missing Out*), que conduce a las personas a revisar constantemente las diferentes cuentas para no quedar fuera de algún evento o actividad social mediada que otros puedan estar viendo o que los pueda estar divirtiendo; según se refiere, *Snapchat* es la red que más provoca este temor.

Este mismo estudio destaca cómo la posibilidad que dan las redes sociales de comparar constantemente imágenes puede incidir en la constitución de la imagen propia, la expresión del sí mismo y la identidad personal, principalmente por la constante comparación de las imágenes propias frente a las que otros comparten. Se ha indicado que la vulnerabilidad se da en este caso por las características propias del periodo adolescente en donde se es más sensible a la aceptación o rechazo social y a la opinión de los demás; al postear una imagen se tiende a hacer con una intención usualmente fundada en la valoración que se hace del Otro como referente, lo cual implica sobrevalorarlo y poner menos atención al sí mismo. El estudio indica que, en orden descendente, *Instagram* es la red social más dañina en este sentido, seguida por *Snapchat*, *Facebook*, *Twitter* y, finalmente, *Youtube*.

Como contraparte, es pertinente mencionar de este estudio que estas mismas redes sociales pueden contribuir al desarrollo individual, pero esto depende de la forma como se usen. Así, *Facebook* ayuda también a generar sentimientos positivos hacia otros (uso pro-social), favorece crear una identidad propia y la posibilidad de sentirse apoyado; de igual forma, se indica que promueve el desarrollo de la capacidad de expresión y la afiliación a grupos y comunidades. De igual manera, se encuentra que *Youtube* ha colaborado en generar conciencia social y a combatir los sentimientos de soledad, la depresión y la ansiedad.

Por otro lado, adicional a la posibilidad de interactividad y fomento de relaciones sociales, otros ejes de relevancia se vinculan con el apoyo que las tecnologías hacen hacia la constitución de la identidad y del sí-mismo.

En seguimiento a esta idea, se encuentran otros ejes de estudio en donde se reitera la relevancia que tienen las redes sociales (*Social Networking Sites,* SNS), la comunicación en línea y la auto-presentación como instrumentos para la construcción identidad en las interacciones sociales mediadas. Salimkhan, Manago & Greenfield (2010), al estudiar la red social *MySpace* (la cual se lanzó en 2003 y fue trascendental como antecesora a sitios sociales web tales como Facebook) plantean de forma interesante, cómo los entornos multimedia de las redes sociales adhieren un nuevo lenguaje visual para representar (presentar y auto-presentarse) el *self*. Adicionalmente, se rectifican nociones acerca de cómo a través de los recursos multimedia, y de las fotografías se crea una narrativa visual y multimedia

Una consecuencia negativa de las redes sociales se relaciona con el fenómeno "miedo a estarse perdiendo de algo"

Según la encuesta #StatusOfMind (2017), Instagram es la red social más dañina desde el punto de vista de la salud mental, seguida por Snapchat, Facebook, Twitter y, finalmente, Youtube

para contar algo de sí y algo social, en este caso conectando el pasado y el presente de un "*self* social". Ya desde 2008, Manago, Graham, Greenfield & Salimkhan habían indicado que esta red social provee nuevas herramientas culturales para la construcción de identidad, particularmente en los jóvenes que se encuentran en este proceso de desarrollo, pues se usa para explorar en ella, para establecer comparaciones sociales y para expresar idealizaciones acerca de cómo desearían llegar a ser (sí-mismo ideal). Se indica que la naturaleza pública del *self* (sí mismo) en estos entornos impone mecanismos de retroalimentación por medio de los cuales los jóvenes legitiman su imagen personal asociada al *self*. De igual manera, se hipotetiza que la representación del *sí mismo* asociada a las diferencias de género puede, posiblemente, intensificar las normas de género que se dan en el mundo *offline*. Se sugiere también que la red social *MySpace* introducía un contexto cultural en el cual las normas sociales de interacciones de auto-presentación creaban nuevas formas de experimentación y reflexión acerca del *self* actual y otro posible. *My Space* parece ser una red social que tiende a reificar / cosificar el *self* a partir de través de la representación social o pública. Sucede de forma similar con la publicación de perfiles, los cuales se presentan de forma estereotipada de acuerdo con las normas de lo que se presupone masculino o femenino, todo lo cual afirma el rol que cumplen los entornos virtuales en la constitución subjetiva, y, en este caso de la identidad personal. Estos elementos relacionados con la influencia de las redes sociales en el desarrollo individual se hacen más interesantes cuando, además, se piensa y considera otras nuevas redes sociales, como *Instagram*, cuyo formato visual parece magnificar estos aspectos.

En seguimiento y correspondencia con las situaciones anteriormente expuestas, desde una perspectiva de la psicología clínica y social relacionada con las posibles afectaciones al desarrollo individual, Sherry Turkle (2012) apunta hacia otras dimensiones del desarrollo tecnológico las cuales califica como menos positivas.

En esta exposición, Turkle (2012) se dedica a analizar el impacto de las tecnologías de comunicación móvil sobre la vida en línea de las personas e indica que existe un efecto-paradoja en relación con los usos y efectos que éstas tienen en los individuos, pues, aunque es bien reconocido que facilitan la vida cotidiana, también se comprueba que afectan y alteran las interacciones y rutinas diarias familiares y los esquemas de comunicación interpersonal. En su opinión, el estar siempre "conectados" hace que no se preste completa atención a quien se tiene en frente porque se tiende a estar más al pendiente del dispositivo; esto da pie a que ella se refiera a estas interacciones como "un estar juntos sin estar juntos" (*Alone Together*) porque hay un distanciamiento de lo real material por lo virtual-digital (que, remite también a una realidad pero con otra materialidad); según indica, este alejamiento puede ser selectivo (se ingresa y sale del mundo real material al virtual y se presta atención solo a lo que interesa). Los dispositivos tienen un poder o fuerza psicológica que cambia lo que las personas hacen y lo que son y, para Turkle, cambian la forma cómo nos relacionamos con los demás, e, incluso la forma cómo lo hacemos con nosotros mismos, así como la capacidad de auto-reflexión. En sus palabras, hoy por hoy, "se sacrifica la conversación por la conexión". Afirma que esta situación puede ser más lesiva para el adolescente que para el adulto, ya que en su proceso de desarrollo necesita de relaciones cara a cara para conformarse y constituirse como ser individual. De igual manera, asegura que la vinculación cotidiana e intensa con la tecnología crea "tres fantasías gratificantes":

1) la de poder centrarse y poner atención en lo a cada quien le interese; 2) la de que siempre seremos escuchados; y 3) la de que nunca estaremos solos. Todo lo cual considera clave porque, en su opinión, en el mundo contemporáneo, los seres humanos no saben estar solos: "en el momento en que la gente está sola se pone ansiosa, se inquieta, se aterra", indica, el dispositivo acompaña, crea una falsa ilusión de acompañamiento. Desde su perspectiva, se presenta una paradoja en la que estamos insertos los individuos: la conexión constante e intensa, que, además, desvirtúe el contacto social real crea una especie de aislamiento, y hace que la gente evite la soledad que es requerida para el desarrollo propio. El estar constantemente conectados afecta la capacidad del encuentro propio o con el sí-mismo, lo cual incide también en la capacidad individual de acceder a otros y de generar formas vinculares reales. Así lo indica: "se llega a estar solo si no se cultiva la capacidad de estar solo, de estar separado, de estar con uno mismo".

Lo anterior revela, por tanto, un rol dual particular de la tecnología móvil y sus múltiples funciones y aplicaciones: positivo para la cotidianidad, pero también, el imperativo llamado de atención a la necesidad de modular o moderar las formas en que se hace uso de ella, de forma tal que no se pondere sobrevalorada al individuo y su constitución personal.

Las amenazas a la identidad personal pueden encontrarse relacionadas con el hurto o suplantación de identidad para cometer fraudes informáticos

9.4 TIPOLOGÍA DE LOS RIESGOS Y AMENAZAS A LA SEGURIDAD DE LA IDENTIDAD VIRTUAL

La creación de esquema y una tipología asociados con las amenazas a la identidad virtual personal adquiere importancia por el creciente interés que tiene en el mundo actual la información relacionada con los datos personales en los diferentes ámbitos de acción cotidianos, principalmente, en el financiero y comercial electrónico, pero también -como se ha visto- por los sistemas de información institucionales (para funcionar y actuar como ciudadano). Todo esto implica el paso de interacciones y contenidos que se daban personalmente a intercambios de información en donde una identidad (código, contraseña) toma mayor preponderancia como instrumento porque éste traduce la identidad en información cuantificable relacionada con ella (UNODC, 2013).

Como se planteó anteriormente, existen amenazas por la exposición al mundo virtual relacionadas con afectaciones al individuo, las correspondencias a la salud mental y la constitución de la identidad personal. Pero, hay otros tipos de amenazas que también trasgreden y afectan al individuo, asociadas con el hurto de identidad, también denominado como delito relacionado con la identidad, apropiación de cuenta o robo de cuenta o fraudes informáticos. Otras amenazas se dan con el fin de dañar o lesionar una imagen y extorsionar para obtener dinero, o bien engañar a otras personas para obtener un fin particular. Todos estos tipos tienen que ver con una intencionalidad y fin particular del ciber-delincuente de obtener algo, lesionando a alguien mediante un medio informático, para lo cual se acude a estrategias de ingeniería social y al conocimiento preciso informático. Algunos tipos de amenazas se encuentran tipificados desde la perspectiva legal, en este caso se les considera ciber-delitos.

Se debe además señalar que, en la actualidad, las amenazas son más sofisticadas y hacen uso de la innovación. Según el *Internet Security Threat Report* (ISTR, 2017), el año 2016 estuvo marcado por ataques fuera de lo normal, caracterizados por desfalcos virtuales de millones de dólares, y aparentes manipulaciones electorales a través de las redes sociales (en los Estados Unidos de Norteamérica), e incluso ataques respaldados por países. Por ejemplo, si bien el *e-mail* o correo electrónico es vital para la comunicación, es hoy fuente de disrupción para individuos y organizaciones y se ha llegado a considerar "el arma de moda" (Ver: Figura 9.5).

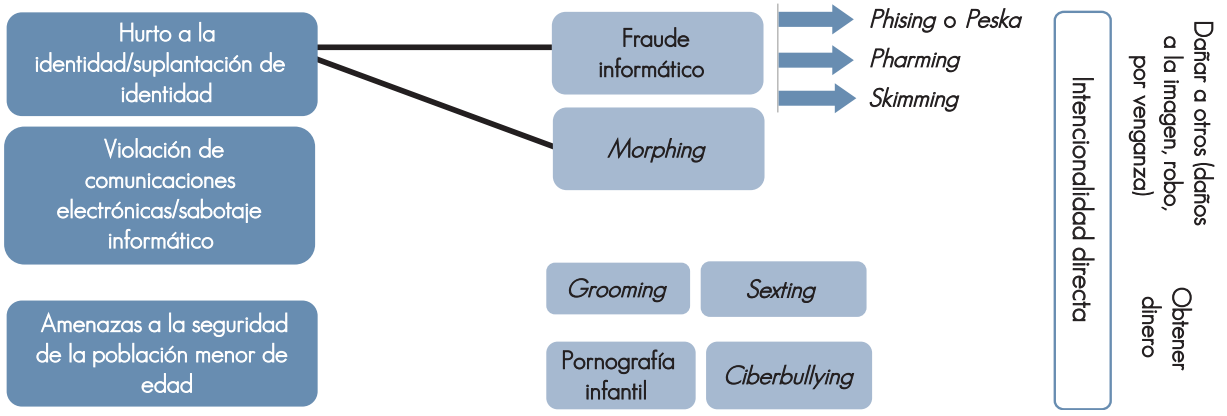

Figura 9.5 Tipología de las amenazas

Fuente: Elaboración propia.

Las amenazas y las formas de cometer delitos tienden a ser cada vez más sofisticadas e innovadoras conforme hay mayor desarrollo tecnológico

Con el fin de establecer una tipología más explicativa acerca de algunas amenazas, se presenta esta información detallada.

9.4.1 Suplantación de identidad

La suplantación de identidad se da con diversos fines: para obtener alguna gratificación personal y hacerle daño a la imagen de otros a través de redes sociales, o bien para obtener ganancias con dinero.

En el primer caso, de la suplantación de identidad a través de las redes sociales, según explica Erick Lewis, Jefe de la Sección de Delitos Informáticos del Organismo de Investigación Judicial (OIJ) (comunicación personal, 18 de setiembre, 2017) se da a través todas las redes: *Facebook, Twitter, Instagram, Snapchat*, en donde se hace una publicación tomando la identidad y el perfil de otra persona con un fin morboso o para hacerle un daño, ya sea enviando un video, una foto o una comunicación que genere algún tipo de conflicto o problema; en este sentido, hace el uso del *Morphing*, que refiere a la transformación de una imagen fotográfica. También se han dado casos en los cuales, se amenaza y extorsiona al dueño del perfil real diciendo que se seguirán haciendo las publicaciones si no responde a sus pedidos, o bien en el caso de adolescentes, se les amenaza y extorsiona diciendo que publicará las fotos para que los papás las vean.

La suplantación de identidad se puede dar a través de las redes sociales, tomando el perfil de una persona y usándolo con algún fin específico. Otras formas de robo o hurto de identidad se dan para cometer fraudes informáticos

De acuerdo con lo que indica Lewis, esto se considera delito si está suplantando a alguna de las personas, o si se utiliza a un tercero, es decir, un perfil falso solo para obtener fotografías y videos. Si es un menor se incurre en un delito, también si hay suplantación haciéndose pasar por un amigo, por ejemplo. Adicionalmente, cuando se trata de un adulto que suplanta una identidad para intercambiar comunicaciones con un menor es un delito, las variantes del mismo se dan según el fin por el cual hace la suplantación, en tal situación, es usual la corrupción de menores por medios informáticos. La segunda situación relacionada con suplantación de identidad se vincula con los fraudes informáticos.

9.4.2 Fraudes informáticos: el Phising (Peska), el Pharming y el Skimming

Uno de los delitos informáticos que se considera más dañino tanto para personas, empresas privadas, o entidades bancarias es el fraude informático. Se indica que, en Costa Rica, entre los años 2007 al 2009 fue el periodo en que hubo mayor cantidad de denuncias por transferencias electrónicas bancarias fraudulentas, principalmente a través de las modalidades de *Phising y Pharming*.

El *Phising*

El *Phising* es considerado un delito cibernético bancario que se activa a partir de un *malware*; no es relativamente nuevo como delito informático y su incidencia en la población costarricense se indica que parece haber aminorado. Mediante este ciber-delito se busca acceder a información confidencial de la computadora de una víctima no específica, a través del correo electrónico o de una página web (Baltodano, 2010) a la que los usuarios de cuentas bancarias se conectan al contestar a un correo electrónico engañoso, pues opera apelando a información y esquemas de comunicación casi reales, como los que recibiría usualmente de parte de un banco. Muy frecuentemente se relaciona con instituciones bancarias en donde se indica a los clientes bancarios que se ha identificado una situación fraudulenta en su cuenta y se le incita a que por lo tanto actualice sus datos. La "pesca" deviene al lanzar "la carnada", que es usualmente una dirección electrónica a la que se pide ingresar; el engaño se da porque este enlace es muy similar a la página oficial de la entidad bancaria, y si la persona logra ser engañada es remitida a una página gemeliada, en donde está reportando su información confidencial. En el pasado se le conocía como "hurto mediante engaño". Hay varias formas de activar este engaño: por medio de llamada telefónica o por correo electrónico.

Uno de los casos más conocidos se relaciona con el Banco Banamex en México, en donde terceras personas se hacían pasar por la institución financiera Citibanamex. El engaño venía dado mediante un comunicado falso por correo electrónico, según el cual, la dependencia informaba al usuario que por motivos de seguridad su cuenta había sido bloqueada y debía realizar la verificación de su identidad en el siguiente enlace: https://boveda.banamex.com.mx/serban/index.htm (el cual era muy similar al del banco). El usuario, al ingresar a la dirección electrónica se le enlaza a un sitio falso, en donde le solicitan datos como el nombre del usuario, domicilio, contraseñas, número de identificación personal (NIP), número de cuenta bancaria de tarjetas de crédito o débito y cualquier otra información particular a un posible delincuente. Este caso se dio en 2017 y ya se habían presentado situaciones similares en otras entidades financieras como HSBC, BBVA y Bancomer.

El phising es uno de los delitos informáticos que más comunes

Costa Rica se considera una "zona tibia" en cuando a la incidencia de ataques cibernéticos con respecto a otros países de Latinoamérica, ocupando el sétimo lugar

La incidencia del *Phising* en Costa Rica se comenzó a revelar más fuertemente desde el 2006 y 2007, años en que se reportan las cifras más importantes. De acuerdo con los datos del Observatorio Judicial, en este momento se reportaron alrededor de 1000 expedientes por año, y muchas de estas causas tuvieron que mantenerse en archivo fiscal por no lograr identificarse al sospechoso ni poder contar con un informe final. Posteriormente, de acuerdo con lo que indica esta misma entidad, se mantuvo para los años 2008 a 2011, alrededor de 300 causas anuales.

Sin embargo, en el país se manifestó una situación relativamente reciente que puso en entredicho la seguridad de la información confidencial de la Caja Costarricense del Seguro Social (CCSS) y reveló la vulnerabilidad del Sistema de Recaudación Centralizada (SICERE). Entre el 13 de marzo y el 26 de mayo del año 2015, la CCSS denunció haber sido víctima de un *hackeo* que comprometió a más de quinientos mil registros de este sistema. Esto se dio cuando se generaron accesos masivos a la base de datos, al usar en el Histórico Laboral "accesos y autenticaciones diferentes de las establecidas, excediendo los privilegios de acceso de datos que usualmente tendría un usuario autorizado". El 13 de marzo de ese año se contabilizaron 37.974 peticiones y el 26 de mayo fueron 151.990 solicitudes de acceso a los servicios de la Oficina Virtual, mientras que el promedio diario es de entre 100 y 200 consultas (Chacón, 20 de setiembre de 2015).

Por otro lado, de acuerdo con Chacón (17 de junio de 2016), en el estudio *ESET Security Report Latinoamérica* del año 2016, se considera a Costa Rica como una "zona tibia" en términos de ataques cibernéticos en relación a otros países de Latinoamérica. Este estudio integró una muestra de 3044 empresas que habían sido afectadas por infecciones *malware* a través del *Phising* en países como Argentina, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Paraguay, Perú y Venezuela; los resultados indican que casi la mitad de las empresas costarricenses fue víctima de ciber-crimen durante ese año. El país que registró más ataques fue Nicaragua (58%) y Costa Rica, con 45% ocupó el sétimo lugar (Tabla 9.1). En este mismo reporte se indica que Brasil tuvo un crecimiento de 197% en ciberataques y que el fraude bancario aumentó un 40% con respecto al año 2014.

El *Pharming*

El *Pharming* es una forma evolucionada del *Phising*, la cual sucede ya con poca frecuencia gracias a la activación de mecanismos de seguridad más efectivos por parte de las entidades bancarias y a una mayor conciencia en la población usuaria.

Tabla 9.1 Cantidad de empresas afectadas por ataques informáticos en países de Latinoamérica (2016)

	País	Porcentaje de Empresas
1.	Nicaragua	58%
2.	Guatemala	55%
3.	Ecuador	51%
4.	Perú	51%
5.	Honduras	50%
6.	Colombia	48%
7.	Costa Rica	45%
8.	El Salvador	41%

Fuente: Elaboración propia, 2018. A partir de Chacón, 2016.

Consistía en el envío de un correo masivo cuyo contenido para atraer a las personas era, por ejemplo, el envío de una tarjeta de felicitación. Al intentar abrirlo se bajaba un archivo virus que, al digitalizar una página electrónica bancaria cambiaba la configuración y remitía a la persona a una dirección falsa, que le permitía al delincuente acceder a la información sobre usuario y contraseña y, por lo tanto, a las cuentas bancarias y realizar transacciones.

La evolución más reciente de este delito es que el virus se propaga desde el correo electrónico, la computadora se infecta y si se utiliza una llave maya, ésta también se infecta, si ésta se usa a la vez en otra computadora el virus se propaga y se maximiza el proceso de infección (E. Lewis, comunicación personal, 18 de setiembre de 2017).

Un caso de *Pharming* remite de nuevo a México, se trataba de un archivo llamado "*videotestimonio.mpeg.exe*" que llegaba hasta el usuario a través de un correo electrónico, y simulando ser una noticia sobre un supuesto secuestro en México. La técnica de engaño es una estrategia de

ingeniería social que se aplica al archivo pues el archivo descargado posee una doble extensión; al ser ejecutado, se abre el navegador predeterminado mostrando una página de *Youtube* (que es lo que por nombre de archivo se esperaba que se abriera), y que se usaba a su vez como estrategia para evadir la atención y evitar sospechas por parte del usuario. Pero, por otro lado, el código malicioso lo que estaba realizando es *Pharming* local que modifica el archivo *hosts* con información maliciosa (*malware*) y que lleva a re-direccionar al usuario de forma implícita hacia un sitio web falso, creyendo que se trata de las entidades bancarias, por ejemplo.

El *Skimming*

Es un tipo de fraude que consiste en copiar la tarjeta de débito o crédito con un dispositivo de lectura de dato para el robo de información en el momento de la transacción, con el fin de reproducir o clonar la tarjeta y hacer uso de ella luego a través del copiado de la banda magnética. Las formas comunes de escaneo, copia o clonaje se dan en lugares públicos, pero sin que la persona se dé cuenta (en gasolineras, bares, restaurantes, o bien, en cajeros automáticos). En este último caso, usualmente se realiza mediante la ubicación de una micro-cámara que permite grabar el código PIN o código de seguridad que la persona marca.

Violación de comunicaciones electrónicas / sabotaje informático

De acuerdo con Erick Lewis (comunicación personal, 18 de setiembre de 2017), se presentan con cierta regularidad delitos informáticos relacionados con la violación de las comunicaciones electrónicas y la alteración de datos y sabotaje informático. Según indica, la incidencia de la alteración de datos y sabotaje informático no es muy alta en individuos, lo cual atribuye a un posible desconocimiento por parte de las personas, y refiere más bien a situaciones en empresas:

> Uno de los casos que tuvimos en una oportunidad fue el de una empresa que recibió un correo electrónico anónimo, donde ofreció las fórmulas químicas de un producto de la competencia. El gerente general de esta empresa alertó a la competencia, se interpuso la denuncia y se inició el contacto con la persona que quería vender la información. Aquí se determinó que el correo provenía de un área específica de la empresa y se logró establecer que la persona que ingresaba, no era el usuario de registro, sino que conocía la clave de la jefatura. Esta persona fue condenada a 6 años de prisión por alteración de datos y sabotaje.

A nivel internacional se encuentran situaciones más recurrentes. Una de las recientemente más conocidas remite al caso de los *Panama Papers* mediante el cual se reveló (filtró) ante el periódico del Sur de Alemania, *Süddeutsche Zeitung*, y el Consorcio Internacional de Periodistas de Investigación (ICIJ), información sobre documentos confidenciales (11,5 millones de documentos, correspondientes a 45 años de datos) de una firma de abogados de Panamá denominada Mossack Fonseca (reconocida como una de las empresas que más sociedades *offshore*[2] registrada en Panamá y con sucursales en todo el mundo: Beijing, Londres, Zurich), relacionados con el ocultamiento de empresas, de activos, y de ganancias, así como con la evasión de impuestos por parte de personas multimillonarias, diversas personalidades de la política mundial, y de otras esferas como las finanzas, el arte y el deporte. Los datos confidenciales incluían informaciones acerca de cuentas bancarias, mensajes de correos electrónicos, hojas de cálculo financieras, pasaportes, registros corporativos de diferentes empresas y jurisdicciones *offshore*.

La incidencia de este tipo de delitos en Costa Rica ha sido fluctuante. Los datos estadísticos del OIJ indican:

- La presencia de 8 casos en el 2007 que disminuyeron a 3 en el 2008.
- En el 2009 la incidencia de 7 casos y de 11 en el 2010.
- El 2011 registró tres casos investigados y en el 2012 registra un caso.

Uno de las situaciones más recientes relacionada con sabotaje informático o violación de comunicaciones electrónicas se relaciona con el caso de los Panama Papers

Otras formas de buscar información personal

Una de las formas refiere al robo de dispositivos informáticos para obtener la información almacenada que muchas veces permanece allí por descuido cuando se trata de equipos de

2 Las sociedades *offshore* se caracterizan por estar registradas en un país en donde no realizan ningún tipo de actividad económica y se benefician de las ventajas fiscales que tienen, por lo que se les considera como paraísos fiscales.

Uno de los aspectos que más dificulta el seguimiento forense a los casos relacionados con el grooming y la pornografía infantil es el temor de la persona menor a hacer la denuncia. Esto es lo que activa la extorsión e inicia el circulo vicioso en que se ve envuelta la víctima

segunda mano (datos confidenciales). Otra forma es la de acceder a buscadores de Internet para obtener información relacionada con la identidad de la víctima (seguir las *cookies* o los sitios web guardados). Se denomina como *Google hacking* o *Googledorks*: se refiere a buscadores que se usan para filtrar la información sobre resultados de búsquedas de la víctima e información personal.

9.4.3 El Grooming o engaño pederasta y la pornografía infantil

Remite a una serie de conductas, acciones o comportamientos ejecutados deliberadamente por un adulto cuyo propósito es ganarse la amistad y generar relaciones de empatía y vinculación emocional con un menor de edad, mediante la coacción o persuasión. Las acciones intencionadas pueden tardar varias semanas o meses y el objetivo primordial es lograr disminuir las barreras inhibitorias de un niño, una niña o un(a) adolescente para lograr que comparta fotografías o videos que luego puedan ser material y objeto de distribución y difusión de pornografía infantil, o bien para hacer incursionar a un menor en la prostitución infantil.

Las acciones del *groomer* se facilitan por el anonimato y la despersonalización que permite Internet, como también por la permeabilidad que se puede facilitar por la mediación (que, en niños pequeños, se pueden ver vulnerados por efecto de la percepción: se le habla a la pantalla de un dispositivo, no a la persona).

Un caso conocido de *grooming* y pornografía infantil se dio en Colombia en el año 2016. Se trataba de un hombre de 23 años quien tenía dos perfiles falsos en *Facebook*, tomando por identidad y a nombre del cantante Maluma (quien es reconocido y afamado por niños, niñas y adolescentes). Mediante la presencia en línea y bajo esta identidad se ganaba la confianza de niñas de entre 9 y 12 años, a quienes les pedía fotografías y videos en las cuales aparecían en ropa interior, o desnudas. Luego de lograr su propósito las amenazaba y extorsionaba diciéndoles que si no accedían a hacer lo que él les indicaba (tener relaciones sexuales con él), iba a publicar las fotos o enviárselas a sus padres. En este caso, se incautaron 15 discos duros, 5 tabletas, 9 celulares, 15 memorias micro SD y 2 memorias USB, que utilizaba para almacenar y distribuir las imágenes[3].

Muchos de estos casos no se resuelven exitosamente debido al temor de los niños (as) al castigo o la reprimenda, pero en otros casos, cuando las víctimas hacen la denuncia, logran dar seguimiento hasta capturar al delincuente. En esta situación particular se logró aprehender al delincuente gracias a la denuncia de una niña víctima frente a su madre, con lo cual logró romper el círculo vicioso de la extorsión.

9.4.4 El Sexting

El *Sexting* se refiere al fenómeno de tomarse fotografías provocadoras y compartirlas con otras personas, usualmente de confianza (Lenhart, 2009, 2010). Este fenómeno inició solamente con el envío de mensajes de naturaleza sexual, y con las posibilidades que permiten los teléfonos inteligentes, evolucionó hacia el envío de fotografías o videos de contenido sexual. Gracias a la permisividad del dispositivo celular para generar intimidad, el *Sexting* (contracción lingüística de *sex y texting*) se ha difundido cada vez más, sobre todo por redes sociales como *WhatsApp* y *Snapchat* que permiten la instantaneidad o inmediatez en el envío de mensajes, fotografías y videos. Particularmente, en el caso de *Snapchat*, al ser una red de mensajería efímera, potencia la participación en este tipo de actividades porque permite perpetuar el inter-juego íntimo-privado vs íntimo-compartido.

La práctica del Sexting se favorece por la permisividad de los dispositivos móviles y de algunas aplicaciones para generar cierta privacidad e instantaneidad, tales como WhatsApp y Snapchat

La práctica del *Sexting* no es en sí un delito informático, llega a serlo cuando se trata de intercambios entre una persona adulta con un menor de edad, o de situaciones que lleven a distribuir o difundir las imágenes o videos para fines pornográficos. Por otro lado, se convierte en una práctica riesgosa y es una importante amenaza a la seguridad e identidad, principalmente para adolescentes o jóvenes, cuando, al no poder medir las consecuencias de estos actos, desconocen el destino final que pueden llegar a tener estas fotografías o videos y afectar su imagen personal, con eventuales consecuencias psicológicas.

3 Ver: http://www.enticconfio.gov.co/tres-casos-grooming-colombia.

Las situaciones relacionadas con el *Sexting* en el individuo que es víctima se viven muchas veces en soledad y tienen consecuencias nefastas, principalmente en los adolescentes quienes, en un afán de explorar el mundo, no logran medir las consecuencias y dimensiones que puede tomar la situación.

El ciberbullying o ciber-matonismo es un subtipo del bullying dado dentro de un espacio cibernético o mediado por algún recurso tecnológico de comunicación automatizada instantánea

Uno de los casos más conocidos es el de Amanda Michelle Todd, una adolescente canadiense quien, a los 12 años, con el propósito de conocer gente nueva, interactuó con un hombre que conoció en *Facebook* y con quien hizo *topless* frente a una cámara web; el hombre la extorsionó para que se desnudara y ante la negativa de ella, compartió las fotografías, terminando en los correos electrónicos de sus compañeros del colegio. Como consecuencia, sus amigos le dieron la espalda, recibió insultos, acoso, marginación social y agresiones por la web, conduciendo a trastornos de ansiedad, depresión y ataques de pánico, al consumo de drogas y de alcohol. A los16 años, el 7 de setiembre de 2012, Amanda decide suicidarse dejando previamente un video en *Youtube* en el cual narró toda su experiencia de chantajes, acosos y agresiones; este video llegó a viralizarse: *Amanda Todd My Story: Struggling, bullying, suicide, seld harm*[4]. Este caso, cuyas consecuencias fueron nefastas remiten a situaciones que, hoy por hoy tienden, lamentablemente, a ser más comunes en el mundo adolescente y en la sociedad contemporánea global, cuyas sus implicaciones, al estar insertas en mundo virtual, son de alta complejidad por todas las dimensiones que integran y por la dificultad de poder controlarlas.

9.4.5 El Cibermatonismo o Ciberbullying

La temática del *bullying* o matonismo trasciende hoy toda frontera, es universal y se relaciona con el fenómeno del *ciberbullying* o ciber-matonismo, el cual tiende a ser aún más complejo pues se acrecienta cuando se viraliza, conllevando a formas de control más difíciles de manejar por las formas de anonimato y despersonalización que permiten los formatos digitales.

Se reconoce el *ciberbullying* como un subtipo del *bullying* o matonismo que se da dentro de un espacio cibernético o mediado por algún recurso tecnológico de comunicación automatizada instantánea (Celada, 2014, p. 70). Esto integra: "el uso de medios telemáticos como Internet, telefonía móvil y videojuegos *online*, para ejercer acoso psicológico entre iguales" (Cyberbullying, 2013; citado por Celada, 2014, p. 70). Esto contiene primordialmente el uso de foros, *blogs, chats,* juegos en línea y redes sociales.

Las formas de abuso dadas mediante el *ciberbullying* refieren usualmente a agresiones, discriminación, humillaciones, amenazas e intimidaciones y al *flaming* (envío de mensajes insultantes o provocadores) mediante los medios electrónicos, las cuales suelen ser anónimos y reiterados, por lo que, una de las dificultades respecto de esta problemática es que muchas veces, las víctimas no reconocen las acciones que se le relacionan.

Las situaciones relacionadas con el *bullying* y el *ciberbullying* han adquirido en la actualidad dimensiones de gran relevancia, en tanto es un fenómeno que se presenta de forma cotidiana en muchos contextos de vida de los adolescentes, poniendo en evidencia un problema de violencia y agresión sociales más amplio al que se debe prestar atención. Enseguida se retoman algunas de las características comúnmente relacionadas con el ciber-matonismo.

En la actualidad, tanto el bullying como el ciberbullying han adquirido dimensiones de gran relevancia, pues se presentan como fenómenos de la vida diaria en muchos adolescentes costarricenses

4 Para mayores referencias, ver: https://www.youtube.com/watch?v=jDvKm_5QbHA).

Tabla 9.2 Características del ciberbullying

Características
Demanda conocimiento y dominio del uso de las TIC, en cualquier tipo de dispositivo, incluyendo juegos mediante consolas en línea.
Es una forma de acoso indirecta, no se da de frente (y muchas veces, se da de forma anónima).
Es un acto de violencia camuflada, el agresor suele ser desconocido, se camufla mediante un "alias" y oculta su verdadera identidad.
El desconocimiento del agresor magnifica el sentimiento de impotencia
Contiene diversos tipos de acoso a través de las TIC: insultos electrónicos, hostigamiento, denigración, suplantación, develamiento y sonsacamiento (buscar información de la víctima para usarla en su contra y humillarla, exclusión, ciber-persecución (el acoso de extiende al uso de diversos medios electrónicos, incluso fuera de Internet y por llamadas telefónicas).
Hay un desamparo legal de estas formas de acoso, ya que, aunque se cierre una web, otra se puede abrir (las páginas web, si bien se pueden cerrar luego de ser reportadas, pueden "renacer" con otro nombre, pero lesionando a la misma víctima o bien a otras.
El acoso invade otros ámbitos de la vida privada y aparentemente seguros como la familia, esto genera la sensación de falta de redes y total desamparo.
El acoso se hace público, se extiende y viraliza rápidamente; mientras que la persona acosada se silencia y encierra.

Fuente: Elaboración propia, Prosic, 2018. A partir de Celada, 2014, pp. 72-73.

9.5 RIESGOS Y AMENAZAS A LA IDENTIDAD PERSONAL-VIRTUAL EN EL CONTEXTO COSTARRICENSE

De acuerdo con los datos generados para el 2015 por la Encuesta Actualidades a nivel nacional, de la Escuela de Estadística de la Universidad de Costa Rica, a través de una encuesta a 1.087 personas con edades de 18 años y más años, se registra que el 67% de la población usa Internet en Costa Rica, de la cual un 94,2% corresponde a población de jóvenes de 18 a 29 años; el 33,7% refiere a personas de 50 o más años.

Se indica en este estudio que la actividad más reportada por los usuarios es visitar redes sociales, páginas personales y chatear, lo cual se registra en un 86,8% de los casos; enseguida se destacan aspectos como la recreación (76,4%). El uso para trabajar o estudiar se registra en 74,8% y enviar y recibir correos en un 71,2%. Otras actividades relacionadas con las compras *on line* y con transacciones bancarias se destacan menos, siendo de 30,7% y 38,4%, respectivamente.

La investigación reporta de manera interesante datos sobre las diferentes formas de victimización *on line* que las personas indican haber vivido, señalándose que el 44,6% del total de usuarios de Internet registrados en el estudio ha recibido algún tipo de amenaza en línea, lo cual parece ser más frecuente en las personas que aparecen más activas (o que hacen uso intensivo de la red), es decir, jóvenes de 18 a 29 años (54,0%) y universitarios (48,7%). Asociado con lo anterior, el informe destaca que al comparar a usuarios de Internet que han tenido algún tipo de amenaza y no los que no las han tenido con la intensidad de uso que hacen de la red (categorizada en bajo, moderado e intensivo) se encuentra que en un 46,8% las personas victimizadas usaron de forma más intensiva la red, comparativamente con un 38,1% que no lo fueron.

Así, en este estudio se reporta que 25,3% ha sido acosada a través de la red, un 11% a 13% han experimentado estafas a través de cuentas de correo electrónico, o han enfrentado problemas por algo que alguien publicó en redes. Y, un porcentaje menor al 6% manifiestan haber percibido daños a la imagen o reputación por publicaciones en redes, haber perdido oportunidades por algo publicado o haberse expuesto a peligros.

En general, los datos sobre delitos informáticos o cibernéticos han tenido mayor incidencia en Costa Rica, desde los años 2006 y 2007, del 2008 y hasta el 2011 el número de causas activas en la Fiscalía, por fraude informático se mantuvo en un promedio de 300 anuales, y es desde 2010 que hay un reporte más sistemático de delitos por parte de la Sección de Delitos Informáticos del Organismo de Investigación Judicial a partir de denuncias realizadas; se indica, además, que es desde 2015 que ha habido un aumento considerable de denuncias a nivel nacional.

Según una encuesta del 2015 realizada a personas usuarias de Internet a nivel nacional, el 44,6% ha recibido algún tipo de amenaza en línea, lo cual se da de forma más frecuente en personas que hacen un uso más intensivo de la red (jóvenes de 18 a 29 años (54,0%) y universitarios (48,7%)

En la actualidad en Costa Rica se identifican casos relacionados con instituciones y empresas, pero también directamente vinculados con personas.

En este sentido, se enuncian casos relacionados con la infiltración de *malware y ransomware;* este último es un programa informático malicioso que encripta toda la información contenida en una computadora y para obtenerla solicita un rescate a cambio. El *ransomware* más conocido recientemente es *WannaCry* que es un ataque generalizado es decir, no focalizado hacia instituciones o empresas específicas, sino que cualquier instancia o persona a nivel mundial puede verse afectada por la violación de comunicación electrónicas, la suplantación de identidad y las estafas informáticas a nivel bancario. Según indica el Director de la Unidad de Delitos Informáticos del OIJ, Erick Lewis (comunicación personal, 18 de setiembre de 2017), los delitos de este tipo han ido evolucionando con el desarrollo de la Internet y el acceso a más dispositivos móviles. Adicionalmente, las estrategias para lograr conectarse con las víctimas se han vuelto más sutiles y sofisticadas y recurren a la ingeniería social; siendo así, se articula una ecuación altamente eficaz de acceso a la víctima: ganándose su confianza para lograr su apertura y mediante herramientas técnicas y tecnológicas para lograr concretar el delito.

De acuerdo con los reportes del Organismo de Investigación Judicial (OIJ), para el año 2016, se registró un total de 80 casos de extorsión sexual o *sextorsion* realizados a través de la Internet. Se indica que las denuncias sobre este tipo de delitos iniciaron desde mediados del año 2015 con 21 denuncias registradas, y que, para marzo del 2017, se cuadriplicaron.

Según se ha podido identificar, muchos de los delincuentes se asocian a bandas que operan desde el extranjero, y el perfil de las víctimas es principalmente hombres profesionales, de 25 a 35 años, usualmente casados (60% de los casos registrados) quienes se toman como víctimas. Los delincuentes crean un perfil falso (usualmente a través de *Facebook*) en el cual una mujer les envía una invitación, para entablar una relación de amistad que luego derive en una interacción sexual virtual, la cual graban por *Skype* sin que la víctima lo perciba y que sirve luego como objeto para lograr la extorsión.

Según expresa Lewis, no hay un patrón definido de las víctimas, ni de los montos de la extorsión, pero, además del costo emocional por el daño a nivel social, laboral y familiar que puede recibir la persona afectada, las extorsiones son, usualmente, por sumas de dinero que van desde los cien a los cinco mil dólares (E. Lewis, comunicación personal, 18 de setiembre, 2017).

Para realizar este tipo de delitos, los delincuentes han estudiado en detalle el perfil de la víctima, usualmente analizando la información que se encuentra accesible en la misma web, lo que les permite conocer y acceder al contacto de los familiares, amigos y personas del trabajo, con lo cual logran el objetivo de activar la amenaza. Como patrón de identificación regular se encuentra que lo usual para este tipo de delitos es que se recurra a la creación de perfiles falsos (generalmente de mujeres y principalmente a través de *Facebook*) para atraer a hombres; estos perfiles tienen una corta duración en Internet (con un máximo de dos días de creados) y, usualmente se percibe que son personas que tienen pocos amigos en la red.

En Costa Rica, los casos de delitos informáticos se dan tanto a instituciones y empresas, como a personas. Las estrategias de engaño son cada vez más sofisticadas y evolucionadas, acudiendo al uso de la ingeniería social.

9.5.1 Riesgos y amenazas a la seguridad e identidad de las poblaciones menores costarricenses

Un eje de relevancia y pertinencia en cuanto a las tecnologías digitales y los dispositivos móviles tiene que ver con el uso que hacen los niños, niñas y adolescentes en Costa Rica; cada vez es más accesible y extendida su utilización y la apropiación que de ella hacen las poblaciones menores de edad.

Según estadísticas del OIJ, en el 2016, hubo un total de 80 casos de extorsión sexual o sextorsion realizados a través de Internet

Los datos más actualizados para la población adolescente en Costa Rica (Pérez Sánchez, 2016), revelan un panorama contextual acerca del uso de las tecnologías reportado para esta fecha. Se indica que la mayoría de los adolescentes tiene acceso a computadora (90%) y a Internet en casa (87,6%). El uso de TIC ocupa un lugar importante en el consumo del tiempo libre y casi la totalidad de la muestra indica poseer un teléfono celular (98,9%) y es su principal tecnología para el acceso a Internet. Es importante indicar que este uso se asocia más al envío de mensajes (4,76%, en un índice de 1 a 5), al uso de Internet (4,69%, en un índice de 1 a 5). El ingreso a redes sociales se reporta alto (4,31% en un índice de 1 a 5), al igual que ver videos en la Internet (4,07% en un índice de 1 a 5) y el envío de fotografías por redes parece darse menos frecuentemente (3,66% según un índice de 1 a 5). Por otro lado, es destacable que las aplicaciones más utilizadas por esta población son *Facebook* y *WhatsApp*; la primera enfocada mayormente hacia un uso pro-social, para la búsqueda de información sobre el país y el mundo, y en un uso menor hacia la expresión de emociones, estados de ánimo y la narración de experiencias personales íntimas.

Esta información es particularmente importante analizarla no solo por la amplitud en el acceso que hay de las tecnologías, sino también por la apropiación que hacen los jóvenes de ellas en los diferentes espacios y actividades de la vida cotidiana y por su papel en la construcción de la identidad individual, como estructurantes de las tareas del desarrollo en esta etapa del ciclo vital. Las características propias y particulares del desarrollo adolescente hacen que ellos sean más propensos a usar estas tecnologías como forma de enlace social, entretenimiento y acceso a conocimiento e información. Como lo comenta Pérez Sánchez (2016), en esta edad se da una mayor apertura a los grupos de pares, lo cual conlleva a formas múltiples interacción que facultan diversos formatos para comunicarse, para establecer relaciones interpersonales, para socializar, y para favorecer medios para la integraciónn social (Pérez, 2011), así como usos informativos, escolares y los propiamente tecnológicos. Así, la comunicaciónn instantánea, las posibilidades que permiten las redes sociales de entablar intercambios comunicativos (mediante imágenes, fotos, *emoticons*, etc.), y el acceso universal a información de todo tipo, hace que los dispositivos móviles sean parte inherente de la vida cotidiana, en los diferentes entornos de desarrollo y convivencia. Esto destaca el papel potencial de la Internet y las TIC como herramientas para favorecer o promover el desarrollo socio-individual en esta importante etapa del ciclo vital.

Es igualmente relevante la comprensión de la dinámica e injerencia cotidiana de las tecnologías digitales y lo que posibilitan en aspectos tales como la construcción de la identidad y la evaluación del sí mismo. En Costa Rica, Pérez, Rumoroso y Brenes (2009) destacaron una investigación relacionada con la tenencia mediática y el uso que de ellas hacen los adolescentes en su tiempo libre, vinculados con la auto-valoración del sí mismo. En este estudio, destacan que el uso de las TIC en el tiempo libre se relaciona positivamente con el bienestar psicológico y contribuye con el desarrollo psicosocial al favorecer la integración social. Adicionalmente, se encuentra que el uso intensivo de las tecnologías orientadas al entretenimiento es una forma de autoafirmación y de valoraciónn positiva (Pérez, 2011).

Como se ha destacado, el acceso y uso intensivo de las TIC en los menores implica el acceso a un mundo amplio, muchas veces novedoso y muy atractivo. Amplifica el espectro de posibilidades y de oportunidades en cuanto a esquemas de comunicación, intercambios y relaciones con personas, así como formas nuevas de acceder al conocimiento, y posibilidades de aprendizaje en múltiples formas y modalidades, esto es sin duda favorable y propio de la Sociedad de la Información en el mundo (SIC) contemporáneo, pero también -como se indicó- implica riesgos. En virtud del propósito que fundamenta este capítulo, resulta pertinente destacar también que, hoy por hoy, la tenencia, acceso y apropiación de las tecnologías, tanto como a la Internet, refleja también una perspectiva que se podría considerar menos positiva.

La Internet y las TIC tienen un papel preponderante como herramientas promotoras del desarrollo socio-individual en niños, niñas y adolescentes, pero según su uso, pueden representar también una amenaza para las poblaciones menores

Ya desde 2010, en un antecedente presentado por Grillo y Esquivel dentro de un compendio de publicaciones elaborado por el Programa Sociedad de la Información y el Conocimiento (Prosic) se advierte la preocupación por el efecto que la acelerada incorporación y uso de las TIC podría tener en los adolescentes, particularmente en aspectos como la formación de la identidad, la conformación de valores, la creación de aspiraciones y formas de relacionamiento social (p. 83). El documento hace un llamado de atención sobre la preminencia de un problema vinculado con la triada: adolescencia-ciberespacio-violencia. En este sentido, es relevante cuestionar la posible exposición a la que la población menor de edad se enfrenta como usuaria,

muy a pesar de sus competencias digitales y tecnológicas. Las amenazas y riesgos refieren a expresiones de violencia en el ciber-espacio (Grillo, Durán y Esquivel, 2009), asociados a la violencia sexual y la pornografía, al *Sexting*, al *Grooming*, al *Morphing*, al *Flaming* y al C*iberbullying*, así como la exposición a mensajes y narrativas que circulan en la web y que proyectan y viralizan tramas como "*13 reasons why*" o el fenómeno *"Ballena Azul*[5]".

Algunos de los riesgos y amenazas han estado vinculados con la transmisión de series de Netflix como "13 reasons why" o el fenómeno denominado "Ballena Azul", el cual incitaba a los adolescentes a retos y a conductas límite que atentaban contra sus vidas

Según Álvarez, Rodríguez y Cuevas (2009) el aprendizaje se facilita por dos vías: de forma autodidacta y mediante los pares, pero algo importante es que los adolescentes poseen mucha confianza en el uso que hacen de las tecnologías, lo cual puede resultar como un beneficio, pero puede también convertirse en un perjuicio cuando hay un exceso de confianza, pues el conocimiento tecnológico y digital no necesariamente se asimila o desarrolla paralelamente a la capacidad de poder valorar y anticipar situaciones que puedan eventualmente transgredir o amenazar la seguridad personal, por la exposición que puede implicar el uso de Internet y las redes sociales. Principalmente porque las competencias digitales en esta edad y el exceso de confianza pueden derivar en que disminuya la prevención, las estrategias de protección, y que, por lo tanto, aumente el riesgo (Grillo y Esquivel, 2010). Esto conlleva a comprender que la Internet y todas las posibilidades que contiene implican repensar las conductas que su uso debe gestar y desarrollar de forma simultánea; es decir, en conductas de uso seguro y responsable o de forma contraria, en conductas riesgosas en estas poblaciones.

Estos mismos autores (2010), retomando a Livingstone (2003) refieren algunas de estos peligros, aludiendo a manifestaciones que desde esa fecha podrían estarse dando:

> Tipos de contenido asociados con la explotación sexual y no comercial; la apología de la violencia como medio para resolver conflictos; el racismo y la homofobia; la amenaza a la privacidad o a la propiedad; y la exposición a una comercializaciónn indiscriminada. (p. 83).

Los antecedentes de estudio en Costa Rica sobre la niñez y la adolescencia en relación con las consecuencias negativas de los usos de las tecnologías y la interactividad en el ciberespacio refieren a estudios realizados por Pérez Sánchez (2013, 2016) con estas poblaciones, y de forma más reciente, a un sondeo realizado por la Universidad Nacional de Costa Rica (2017).

En el año 2013, este autor presenta los resultados de una investigación que realizó junto con el Prosic dirigida principalmente a estudiar los usos del Internet, de los video juegos y las redes sociales, así como de la organización del tiempo libre y la tenencia de tecnologías en una muestra de 422 niños y niñas, con una edad promedio de 11,1 años, de escuelas públicas y privadas del área metropolitana. Como aspecto pertinente para el objetivo de este capítulo destaca el interés por medir las variables predictoras del ciber-matonismo y la ciber-victimización en esta población. Entre algunos de los resultados más relevantes, se identifica que el ciber-matonismo o *ciberbullying* está asociado con la intervención parental permisiva, particularmente: el tipo de mediación tecnológica en la que los padres/madres no intervienen en su uso, y la utilización intensiva de *Facebook* tienden a favorecer la presencia de conductas asociadas a ciber-matonismo en niños; por otro lado, la ciber-victimización se predice por la intensidad de uso de *Facebook.* Se precisa igualmente, que aquellos entornos en donde hay una mediación orientada hacia la guía y acompañamiento por parte de padres y madres habrá menos presencia de ciber-matonismo.

Las investigaciones sobre las consecuencias negativas de los usos de las tecnologías y el Internet en Costa Rica en personas menores han estado primordialmente enfocadas en el estudio del ciberbullying y la ciber-victimización

Una perspectiva más reciente (Pérez Sánchez, 2016), y realizada con una muestra costarricense

5 Ballena Azul o *Blue Whale* es un fenómeno de las redes sociales y Internet que comenzó siendo un juego en el año 2015, con las primeras referencias al mismo en algunas regiones de Rusia. El "juego" consiste en una serie de desafíos o retos de diferente naturaleza, que grupos de les redes interponen individuos (debe realizar uno por día durante 50 días), pero que buscan confrontarlo consigo mismo y situaciones que usualmente generan temor, y que bajo un efecto ascendente, confrontan la vida con la muerte. Por ejemplo: levantarse de madrugada a ver videos de terror, cortarse un brazo…hasta llegar al desafío 50 que reta a lanzarse del borde de un balcón. El fenómeno comenzó a desatar muertes en varios países (Rusia, México, Brasil, Colombia) y ya en abril 2016 generó un estado de alarma general. Se cree que los "grupos de la muerte" que incitaron a esta actividad se crearon en la red social rusa VKontakte, y según el primer medio de comunicación que registró esta situación (Novaya Gazeta), de noviembre 2015 a abril 2016, se suicidaron 130 niños y adolescentes en ese país.

de adolescentes (n= 628), estudiantes de colegio público y privado, de zona urbana y rural, cuya edad promedio era de 15,7 años, identificó que tanto el *bullying* como el *ciberbullying* son una realidad presente en la cotidianidad de los jóvenes. Si bien el 21,7% de la población consultada indica no haber realizado acciones referidas al matonismo, un 58% afirma haber manifestado esporádicamente conductas relacionadas con el ciber-matonismo. De igual manera, aunque un 28,8% de la muestra consultada indicó no hacer sido víctima de *bullying*, un 57,5% sí señaló haber sufrido *bullying* cibernético alguna vez. Destaca igualmente, que un 2,7% de la población encuestada expresó sufrir *ciberbullyin*g con una alta frecuencia.

En esta misma investigación, Pérez Sánchez (2016) hace una indagación en ciertas medidas sobre ciberseguridad. El interés se enfocó en las percepciones de los jóvenes acerca de sus propias conductas de protección y seguridad cibernéticas. El autor precisa datos relacionados con las conductas o actividades riesgosas asociadas a la protección de la computadora, el manejo de la privacidad o las búsquedas seguras de información. Los resultados indican que existe baja preocupación por la seguridad y protección de la información/comunicación que se recibe de Internet (70,9% no modifica las preferencias de búsquedas seguras en el *browser;* un 78% nunca ha buscado información para mejorar el uso seguro de Internet; casi un 50% borra el registro de búsquedas del Internet. Pero, por otro lado, sí se rectifica que la mayoría (60,5%) modifica la configuración de privacidad de las redes sociales o la mensajería, y un 73,4% bloquea a personas con las que no se quiere comunicar, o un 62,6% bloquea anuncios y correos indeseables). Se evidencia una relativa preocupación por la seguridad de la comunicación proveniente de Internet, pero también se refleja que los adolescentes no ponen suficiente atención a la revisión de fuentes, al manejo de la privacidad o al cuidado y protección de virus informáticos.

Sobre este mismo tema, un estudio más reciente reporta datos a marzo del año 2017[6] e indica que los estudiantes más propensos al ciber-acoso en Costa Rica son los de sétimo, octavo y noveno, al considerarse que probablemente a esa edad aún no han recibido o adquirido destrezas y herramientas para hacer frente a este problema. Esta reseña se basa en los datos de un estudio realizado por el Centro de Investigación y Docencia en Educación de la Universidad Nacional de Costa Rica, en donde participaron estudiantes de colegios de Heredia y Coronado, y se indica: El 23,7% de los estudiantes de sétimo, octavo y noveno reconocieron haber sido víctimas de *ciberbullying* alguna vez, con consecuencias importantes en la motivación y concentración hacia los estudios. Mientras que en los estudiantes de décimo y undécimo se refirió esto en un 16,9%, pero con impacto a nivel emocional y social; por otra parte, un 83,1% de los estudiantes negó haber sufrido *ciberbullying*.

Por otra parte, se ha encontrado que, en general, la capacidad de seguimiento a los delitos en donde hay menores de edad involucrados, tales como el *Grooming* o engaño pederasta, el *Sexting* o la pornografía infantil, tiende a ser incipientes, justamente por la condición de vulnerabilidad de estas poblaciones, porque se les persuade o extorsiona con menos dificultad o porque no le cuentan a sus padres/madres las situaciones que transitan por temor al regaño o el enojo de ellos. No obstante, según indica Lewis (comunicación personal, 18 de setiembre de 2017), los casos parecen ir en aumento.

Otro tema de amplia relevancia en Costa Rica es la pornografía infantil. Ésta se ubica como el delito informático que más aumento de casos ha tenido en los últimos años en Costa Rica, registrando para inicios del 2017 aproximadamente 50 casos reportados por la Sección de Delitos Informáticos del Organismo de Investigación Judicial. De acuerdo con lo que se indica, en la mayoría de los casos se evidencia con claridad que la Internet se utiliza como medio para la difusión, producción, y, principalmente intercambio de videos de material con pornografía infantil lo cual se da mediante el funcionamiento de foros y plataformas digitales.

La pornografía infantil es el delito informático que ha tenido un incremento mayor en el número de casos reportados a inicios del año 2017

Los situaciones más recientes relacionadas con la pornografía infantil en Costa Rica registrados son de inicios del año 2017, con el hallazgo de al menos cinco casos que involucraron a bebés con menos de un año de edad; y, a mediados del año, con la detención de tres sujetos, quienes no se conocían físicamente, pero compartían en un grupo de *WhatsApp* fotografías y videos de niños menores de 10 años teniendo relaciones sexuales forzadas con adultos; el material no era producido en Costa Rica pero sí distribuido en el país. A los hombres se les arrestó acusados de distribuir, exhibir y difundir material pornográfico a través de esta aplicación. Otros casos graves se dieron en el año 2009, cuando se detuvo a fotógrafos con grabaciones de violaciones de más de 26 menores de edad en este año[7].

6 Ver: https://www.nacion.com/ciencia/salud/colegiales-de-7deg-a-9deg-son-mas-propensos-a-sufrir-ciberbullying/YS6HAAN7RDQNEVWAANFETHFN4/story/

7 Ver: http://www.crhoy.com/nacionales/guerra-contra-porno-infantil-casos- en-el-pis-no-acaban/; www.repretel.com/actualidad/pornografía-infantil-crece--costa-rica-79753).

9.6 MARCO LEGAL SOBRE LOS DELITOS INFORMÁTICOS EN COSTA RICA

La digitalización acelerada de la sociedad condujo a que se diera una reforma relativamente reciente (2012-2013) del marco regulatorio de los derechos de la personalidad virtual

En primera instancia, sobre este tema particular, cabe mencionar que el derecho informático en Costa Rica es una disciplina de aplicación reciente, la cual se ha ido desarrollando de forma paralela al crecimiento de la Internet y las TIC, pues, dado el aumento de riesgos y amenazas, ha sido necesario crear un marco legal para la protección de la sociedad.

El derecho informático tiene un rol importante dentro de la SIC o Ciber-sociedad (como también se le ha llamado); desde esta disciplina, la informática es instrumento y objeto de estudio, en donde también se destaca la figura de la *personalidad virtual*. Esta se define como una identidad inmaterial que integra o contiene datos del individuo en Internet. Sobre este punto, es importante indicar, de entrada, que la personalidad material sí ha tenido una regulación en la Carta Magna costarricense, pero su contraparte en la personalidad virtual ha carecido de legislación (Celada, 2014). La digitalización acelerada de la sociedad ha implicado, recientemente, una reforma en el marco regulatorio acerca de los derechos de la personalidad virtual, también denominados *"derechos fundamentales 'virtuales'* " (p. 42), por lo cual se ha generado un desarrollo incipiente, promovido, justamente por la evolución de las TIC, y por el aumento de riesgos y amenazas informáticos en la SIC.

Celada (2014) también informa que existen diferentes tratamientos al término *Derecho Informático;* al ser una rama del Derecho relativamente nueva, su conceptualización se ha ido modificando a lo largo de los cambios sociales. Thompson Reuters (2013, citado por Celada, 2014) ofrece una definición general del Derecho Informático, refiriéndolo como:

> El conjunto de normas jurídicas que regulan la utilización de los bienes y servicios informáticos en la sociedad, incluyendo como objeto de estudio: 1) el régimen jurídico del software; 2) el derecho de las redes de transmisión de dato; 3) los documentos electrónicos; 4) los contratos electrónicos; 5) el régimen jurídico de las bases de datos; 6) el derecho de la privacidad; 7) los delitos informáticos; y, 8) otras conductas nacidas del uso de los ordenadores y de las redes de transmisión de datos (p.43).

Siendo de primordial interés para este documento la referencia al numeral 7, que versa sobre el entendimiento de los delitos informáticos.

9.6.1 Los delitos informáticos

Acentuar una única definición sobre el delito informático no es posible. De acuerdo con Celada (2014) remite a un marco conceptual amplio, pero que integra de forma muy general, varios componentes fundamentales, tales como: comportamientos criminógenos, atípicos, ilegales; uso de tecnología informática como instrumento, o un proceso de transmisión de datos, un sujeto activo (delincuente) y un sujeto pasivo (la víctima).

Celada concluye definiéndolo como una "acción delictiva realizada por un sujeto (activo) utilizando un medio informático con el objetivo de lesionar los derechos del titular informático (sujeto pasivo -víctima-), de un hardware o software, mediante la acción denominada ciberdelincuencia llevada en un lapso corto" (p. 46). La víctima se concibe como un sujeto pasivo que ha sido violentada en su personalidad virtual. El delincuente informático se concibe como un sujeto activo, y se indica que "no se trata de un delincuente común" (p.47) pues se le adscriben competencias y conocimientos particulares.

El marco jurídico sobre los delitos informáticos en Costa Rica implicó primeramente el entendimiento del desarrollo y consolidación de una normativa a nivel internacional, que luego llegó a Costa Rica

9.6.2 Marco histórico de la legislación del delito informático

El estudio del marco jurídico sobre los delitos informáticos en Costa Rica, conduce primeramente al entendimiento del desarrollo y consolidación de una normativa a nivel internacional que luego llegó a Costa Rica. En general, se revela un tránsito histórico hacia la definición de una legislación y tipología de los delitos informáticos relacionados con la identidad, que integra acciones de diferentes organismos e instituciones internacionales. Este proceso se puede visualizar en la siguiente síntesis.

Tabla 9.3 Proceso para el desarrollo de un marco jurídico

Año	Procesos y acuerdos	Relevancia
1999	Consejo de la Organización de Cooperación y Desarrollo Económicos (OCDE) aprueba un conjunto de directrices para la protección del comercio electrónico.	Generación de estrategias para prevenir el hurto de identidad, pero las estrategias no tuvieron carácter vinculante para tipificar hurtos de identidad.
2001	30 países miembros del Consejo de Europa firman el Convenio sobre el delito cibernético del Consejo de Europa, incluyendo 4 países no miembros que participaron en las negociaciones: Canadá, Estados Unidos de América, Japón y Sudáfrica.	
2003	La OCDE elabora un marco amplio para llevar a cabo investigaciones que permitieran procesar delincuentes.	Se avanza en acciones pero no se puede concretizar una tipificación de hurtos de identidad.
2005 (16, dic)	Se aprueba en Asamblea General de las Naciones Unidas la resolución 60/177 relacionada con la Declaración de Bangkok sobre "Sinergias y respuestas: alianzas estratégicas en materia de prevención de delito y justifica penal" .	Enfatizar la importancia de combatir la falsificación de documentos de identidad para frenar la delincuencia y la organización terrorista.
2007	EN la Resolución 2004/26 del Consejo Económico y Social (ECOSOC), la UNODC desarrolla un estudio sobre fraude y falsificación de identidad y uso indebido con fines delictivos.	Expresa directamente información sobre delitos relacionados con la identidad, abarca toda conducta relacionada con hurto y falsificación de identidad. Integra todos los actos de hurto de la identidad cometidos por medio de Internet como acto delictivo.
2007 Julio, 2007	La Unión Europea ya ha realizado varios instrumentos jurídicos que abordan aspectos sobre la información relacionada con la identidad, tales como la Directiva sobre la privacidad, aspectos sobre fraude y delitos relacionados con Internet y el acceso ilegal a los sistemas informáticos. La Comisión (DG Justicia, Libertad y Seguridad realiza un estudio comparativo sobre las definiciones de la expresión "hurto de identidad" utilizada en los Estados miembro y las consecuencias penales del mismo.	Ninguno de estos documentos consolida disposiciones penales sobre el hurto de identidad (a pesar del reconocimiento de las actividades delictivas). Se rectifica que la cooperación judicial y policial de la UE se facilitarían si se tipificara el hurto de identidad en los Estados miembros.
2007	El Consejo de Europa publica un estudio que analiza los diferentes criterios para tipificar el hurto de identidad relacionado con Internet.	Especifica disposiciones sobre el delito cibernético en casos de hurto de identidad, pero no aplicaciones a actos conexos.
2008	La OCDE publica un estudio sobre el hurto de identidad en línea denominado *Scoping Paper on Online Identity Theft.*	Analiza de forma precisa las diferentes estafas relacionadas con el hurto de identidad realizadas por Internet; aborda aspectos sobre las víctimas y ámbitos de aplicación de la ley.

Continuación Tabla 9.3

Año	Procesos y acuerdos	Relevancia
2008	La OCDE publica un nuevo documento: *Policy Guidance on Online Identity Theft.*	Ofrece un panorama general acerca de las diferentes estrategias para responder al hurto de identidad relacionado con Internet
2008	A los 30 países miembros del Consejo de Europa que firmaron en 2001 el Convenio sobre el delito cibernético del Consejo de Europa, se suman 15 países más. Para esta fecha, 23 países ya lo habían ratificado.	Este convenio tiene disposiciones esenciales para tipificar actos tales como el acceso ilegal a sistemas informáticos o la interferencia de los sistemas. El instrumento es considerado como importante para la lucha contra el delito cibernético y es avalado por diferentes organismos internacionales.

Fuente: Elaboración propia. Prosic, 2018. A partir de Gercke (2009). Documento de trabajo de la tercera reunión del grupo de expertos en delitos sobre identidad celebrada en Viena. Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC, 2013).

9.6.3 Marco legal en Costa Rica

La clasificación de los delitos informáticos es variada a nivel internacional. La legislación costarricense sobre los delitos de este tipo se establece en el Decreto Legislativo Nº 9048, Expediente Nº 17613 "Reforma de varios artículos y modificación de la sección VIII, denominada de Delitos informáticos y conexos, al título VII del Código Penal". Aquí se expone una clasificación de los delitos informáticos, incluyendo reformas que se le han ido haciendo a la legislación. Se tipifica en 7 materias:

1) Delitos informáticos relacionados con la corrupción de menores y su protección;

2) Delitos informáticos relacionados con la violación de correspondencia o de comunicaciones;

3) Delitos informáticos relacionados con la seguridad del Estado;

4) Delitos informáticos relacionados con temas patrimoniales;

5) Delitos informáticos relacionados con el Derecho al honor e imagen;

6) Delitos informáticos relacionados con modificaciones y daños informáticos o de sistemas;

7) Delitos informáticos relacionados con la facilitación delictiva.

La reforma mencionada a varios artículos de este Código Penal (Nº 9048) se llevó a cabo durante los años 2012-2013, la cual consistió en la inclusión de nuevos delitos relacionados con la delincuencia informática. Esto se realizó con el fin de favorecer un mejor abordaje de los casos en Costa Rica.

Esta reforma amplía los alcances de delitos como el daño informático, el daño agravado, el sabotaje informático e incorpora todo un nuevo capítulo dentro del Código Penal, referente a los Delitos Informáticos y conexos, donde se añade la suplantación informática, el espionaje informático, la instalación o propagación de programas informáticos maliciosos, la suplantación de páginas electrónicas, la facilitación del delito informático y la difusión de información falsa.

Enseguida se presenta una síntesis que busca sistematizar la información que contiene estos artículos y los cambios o reformas que han tenido.

Tabla 9.4 Cambios en la legislación a partir de la Reforma de la Sección VIII, Delitos informáticos y Conexos, del Título VII del Código Penal, Nº 9048 de la Asamblea Legislativa

	Tipo de delito	Artículo original	Reforma
1.	Delitos informáticos relacionados con la corrupción de menores y su protección (corrupción, suplantación de identidad)	Artículo 167 del Código Penal sobre corrupción	Artículo 167 bis – Añade: Seducción o encuentros con menores por medios electrónicos[8] Se adiciona por el artículo 2º de la Ley Nº 9135, del 24 de abril de 2013. Publicado el Alcance Nº 78 a la Gaceta Nº 80 del 26 de abril de 2013
		Artículo 230 del Código Penal sobre Suplantación de identidad	
2.	Delitos informáticos relacionados con la violación de correspondencia o de comunicaciones.	Artículo 196 del Código Penal Violación de correspondencia	Artículo 196 bis – **Añade:** Violación de datos personales Se adiciona por la Ley Nº 8148, del 24 de octubre de 2001, reformado en el artículo 1º de la Ley Nº 9135 del 24 de abril de 2013. Publicado en la Alcance Nº 78 a la Gaceta Nº 80 del 26 de abril de 2013.
3.	Delitos informáticos relacionados con la seguridad del Estado	Artículo 288 del Código Penal Relacionado con espionaje, narcotráfico y crimen organizado	Este artículo no sufre una reforma
4.	Delitos informáticos relacionados con temas patrimoniales (extorsión, estafa informática, espionaje informático y difusión de información falsa	Artículo 214 del Código Penal relacionado con la extorsión.	Este artículo no sufre una reforma
		Artículo 217 del Código Penal sobre Estafa Informática.	Artículo 217 bis[9]
		Artículo 231 del Código Penal, sobre Espionaje Informático.	Artículo 231, no sufre una reforma
		Artículo 236, sobre Difusión de Información Falsa.	Artículo 236, no sufre una reforma

8 Será reprimido con prisión de uno a tres años a quien, por cualquier medio, establezca comunicaciones de contenido sexual o erótico, ya sea que incluyan o no imágenes, videos, textos o audios, con una persona menor de quince años o incapaz.

La misma pena se impondrá a quien suplantando la identidad de un tercero o mediante el uso de una identidad falsa, por cualquier medio, procure establecer comunicaciones de contenido sexual o erótico, ya sea que se incluyan o no imágenes, videos, textos o audios, con una persona menor de edad o incapaz.

La pena será de dos a cuatro años, en las conductas descritas en los dos párrafos anteriores, cuando el actor procure un encuentro personal en algún lugar físico con una persona menor de edad incapaz.

9 Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistemas automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.

La pena será de cinco a diez años de prisión, si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

Continuación Tabla 9.4

	Tipo de delito	Artículo original	Reforma
5.	Delitos informáticos relacionados con el Derecho al Honor e Imagen (suplantación de identidad, suplantación de páginas electrónicas)	Artículo 230 del Código Penal, relacionado con suplantación de identidad.	Artículo 230, relacionado con suplantación de identidad, no sufre una reforma.
		Artículo 233, sobre suplantación de páginas electrónicas.	Artículo 233 sobre Suplantación de páginas electrónicas., no sufre una reforma.
6.	Delitos informáticos relacionados con modificaciones y daños informáticos o sistemas (daño informático, daño agravado, sabotaje informático, instalación o propagación de programas informáticos)	Artículo 229 del Código Penal, relacionado con el daño informático.	Artículo 229 bis. –Daño Informático[10]
		Artículo 229 del Código Penal, relacionado con el daño agravado	Se añade inciso 6): "Se impondrá prisión de seis meses a cuatro años (…) 6) Cuando el daño recayera sobre redes, sistemas o equipos informáticos, telemáticos o electrónicos, o sus componentes físicos, lógicos, periféricos".
		Artículo 229, relacionado con el sabotaje informático	Se hacen especificaciones al artículo 229 relacionado con el sabotaje informático.[11]
		Artículo 232 del Código Penal relacionado con la Instalación de programas informáticos maliciosos	
7	Delitos informáticos relacionados con la facilitación delictiva	Artículo 234 del Código Penal, relacionado con la facilitación del delito informático	Artículo 234 del Código Penal, relacionado con la facilitación del delito informático, no sufre reforma.

Fuente: Elaboración propia. Prosic, 2018. A partir de Reforma de la Sección VIII, Delitos informáticos y Conexos, del Título VII del Código Penal, Nº 9048 de la Asamblea Legislativa y de Celada, 2014).

En general, desde el año 2001 se han creado tipologías penales relacionadas con delitos informáticos, pero la normativa jurídica al respecto ha sido "vaga la para la regulación de este tipo de conductas ilícitas", considerando que estas se desarrollan conforme avanza el desarrollo tecnológico y la ampliación de recursos y medios informáticos.

Desde la perspectiva de Roberto Lemaître Picado, abogado-ingeniero informático y especialista en delitos informáticos y temas relacionados con la ciberdelincuencia y ciberseguridad (comunicación personal, 27 de noviembre de 2017), la

10 Se impondrá pena de prisión de uno a tres años al que sin autorización del titular o excediendo la que se le hubiere conferido y en perjuicio de un tercero, suprima, modifique o destruya la información contenida en un sistema o red informática o telemática, o en contenedores electrónicos, ópticos o magnéticos.

La pena será de tres a seis años de prisión, si la información suprimida, modificada, destruida es insustituible o irrecuperable.

11 Se impondrá pena de prisión e tres a seis años al que, en provecho propio o de un tercero, destruya, altere, entorpezca o inutilice la información contenida en una base de datos, o bien, impida, altere, obstaculice o modifique sin autorización el funcionamiento de un sistema de tratamiento de información, sus partes o componentes físicos o lógicos, o un sistema informático.

La pena será de cuatro a ocho años de prisión cuando:

a) Como consecuencia de la conducta del autor sobrevenga peligro colectivo o daño social.

b) La conducta se realice por parte de un empleado encargado de administrar o dar soporte al sistema de red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

c) El sistema sea de carácter público o la información esté contenida en bases de datos públicas.

d) Sin estar facultado, emplee medios tecnológicos que impidan a personas autorizadas el acceso lícito de los sistemas o redes de telecomunicaciones.

nueva legislación y las calificaciones de seguridad en Costa Rica han mejorado. Se considera también que, a nivel de la región latinoamericana, esta nueva legislación sobre delitos informáticos contiene un gran avance e innovación al incorporar delitos como el de suplantación de identidad (el cual se considera muy etéreo pero con efectos visibles en las personas víctimas). La novedad se encuentra no solo en el hecho de incorporar esta figura, sino también en plantear una sanción penal cuando una persona física toma la identidad de otra y la maneja desde un ámbito de redes sociales, páginas web u otros medios de comunicación masiva.

Otro aspecto que se valora como positivo de esta Reforma es que los cambios mejoran aspectos en materia de interpretación de la Ley, lo cual permitiría facilitar la tarea en caso necesario de llevar las situaciones juicio. En opinión de Erik Lewis (E. Lewis, comunicación personal, 18 de setiembre de 2017), esta nueva legislación es más específica y responde a los delitos que se dan en la realidad. Esto lo valora positivo porque sirve de base para favorecer alianzas internacionales en el combate de los delitos, aspecto que es muy relevante para llevar a cabo las investigaciones forenses con éxito.

9.6.4 Otras acciones en el ámbito jurídico

Por otra parte, en cuanto a acciones y avances importantes en el ámbito jurídico, se deriva la existencia de otras leyes que tienen relación e injerencia actual en el marco del uso de la información personal contenida o transmitida mediante medios informáticos o redes sociales.

Desde el marco de la Constitución Política, se habla de la protección de datos personales de los habitantes, de los derechos a la libertad, del secreto de las comunicaciones, e incluso, desde código civil se hacen referencias al derecho a la imagen. De igual manera, en el Código Comercio se alude al secreto bancario. Adicionalmente, un aspecto de relevancia reciente refiere a la protección de datos de los habitantes

En Costa Rica, la Sala Constitucional tiene, además un recurso en términos jurídicos, denominado *Habeas Data* el cual establece las bases jurídicas de la protección informativa; en este sentido indica cuáles son los derechos y obligaciones de todos los habitantes en el tratamiento de datos personales.

El marco normativo acerca del tratamiento de Datos es reciente y se rige desde el año 2011; el mismo está actualmente establecido en la Ley 8968, de *Protección de la Persona contra el Tratamiento de sus Datos Personales* que se crea con el objetivo de garantizarle a cualquier persona el respeto a sus derechos fundamentales de autodeterminación personal, específicamente en el principio de *Autodeterminación Informativa* que garantiza la defensa del tratamiento de su información personal. Este aspecto se volvió muy importante desde el año 2005, en que se da un desarrollo más amplio de la plataforma web y se hace más activa la participación ciudadana; esto ha implicado que la información personal se concibiera como objeto de uso "libre" pues las personas suben y bajan información personal, pero que también ha implicado conflictos, cuando terceras suben información a alguna plataforma sin consentimiento; esto es lo que se denomina como *derecho de autodeterminación informativa*. Éste es un derecho fundamental que se deriva del derecho a la privacidad y responde a la facultad que tiene toda persona para decidir y ejercer control sobre su propia información personal, contenida en registros públicos o privados, no concierne de manera exclusiva los datos almacenados en medios informáticos.

Otras acciones implementadas como marco normativo refieren al tratamiento de datos personales. La Ley 8968, rige desde el año se 2011 y remite a la Protección de la Persona contra el Tratamiento de sus Datos Personales

En este sentido, las personas pueden decidir si esta información puede ser usada, o si la ceden, o bien autorizar a alguien más para darle un tratamiento.

Los datos personales son todos aquellos que se resguardan en físico como en digital, o datos automatizados, tales como bases de datos, archivos de expedientes y tienen un acceso restringido lo cual implica que son únicamente de interés para el titular de los datos y para la administración que los está custodia, esta asume una responsabilidad en el tratamiento de los mismos sin copropiedad.

Los datos se conciben de acuerdo con su naturaleza. Hay datos de *acceso estricto* (datos específicos, contenidos en bases de bases públicas de acceso general, como los datos del Registro Civil, otros son datos de acceso restringido, como el correo electrónico, los datos

para acceder a un seguro, la dirección física, los datos bancarios, el historial crediticio, el historial laboral, la información salarial. En este dominio se encuentran elementos como el nombre completo, la edad, el sexo, la dirección referencial, el estado civil, la fecha de nacimiento, la nacionalidad, la tenencia de propiedades o de sociedades, los teléfonos locales. Otros son los *datos sensibles* que se componen por información más íntima de la persona y que pueden generar algún tipo de discriminación o de alienación social y daño grave a la persona (por ejemplo, los relacionados con la salud, identidad sexual, religión, afinidad política, datos biológicos, historial biomédico, asociaciones gremiales, raza o etnia; algunos de ellos son muy específicos como una imagen o la voz).

Lo anterior es actualmente muy importante, cuando a través de las redes sociales se hace uso libre e indiscriminado de recursos para captan y almacenan registros visuales (fotografías) y de voz (audios), los cuales no solo se generan (toman) sino que se manipulan y comparten. Al respecto, Wendy Rivera Román, Directora Nacional de la Agencia de Protección de Datos de los Habitantes en una conferencia dada en noviembre del 2017, indicó:

> A veces tenemos la idea de qué un dato es la entrada en un registro o un número, pero no una imagen (…). El caso de la foto es delicado, por lo común que se ha vuelto común el compartir fotos, pero (…) si me tomo una foto en una actividad, en una reunión, una fiesta y la subo a las redes sociales y etiqueto a mis amigos (…) se puede volver problemático [indica que, si la persona quiere gestionar sus propios datos de esa manera, es un asunto de decisión personal, pero si incluye o integra elementos sobre la imagen de otras personas, puede convertirse en una situación conflictiva]. ¿Quién autoriza para que yo haga esa utilización de la información, de ese dato personal, si la imagen le pertenece a esas personas?

Este resguardo se vuelve relevante en la medida de que "dato" remite a cualquier aspecto que vincule a la persona y es su derecho. Hoy por hoy esto se vuelve muy importante porque se ha generalizado el uso de fotografías, videos, como recursos no solo informativos, sino también de denuncia a través de las redes; por ejemplo, actualmente, con cierta recurrencia, se dan casos en los cuales se toma una foto a la placa de un automóvil mal estacionado para manifestar molestia, o para lesionar de cierta manera la imagen pública de esta persona al subirla a una red social, éstas se han convertido de alguna manera, en un "tribunal público", pero no se considera que esa persona tiene un derecho sobre su información y si ese acto le daña en cierta medida (puesto que a través de la información sobre una placa de un automóvil se puede tener acceso a otros datos e identificar a su dueño), puede incluso establecer una demanda pues causa daño la intimidad de esa persona.

9.7 CONSIDERACIONES FINALES

La proliferación y el uso de las tecnologías y los dispositivos móviles presenta múltiples beneficios en prácticamente todos los niveles de la sociedad, siendo aprovechada por individuos, grupos, instituciones, comunidades y gobiernos; sin embargo, de la exposición anterior es fácilmente deducible sus potenciales afectaciones negativas, sobre todo de aquellos usos mediados por la Internet y la comunicación *on line*. La argumentación presentada hasta este momento ha puntualizado en algunos aspectos de la sociedad contemporánea y sus estilos comunicativos digitales que conllevan posibles amenazas y riesgos a la seguridad y al resguardo de la identidad personal; principalmente, hemos tratado de mostrar la vulnerabilidad de ciertos sectores y grupos poblacionales.

En el proceso de constitución de la identidad personal, principalmente en etapas del ciclo vital como la niñez y la adolescencia, las relaciones interpersonales son fundamentales para la constitucióonn del sí-mismo en la conformación de la identidad personal. En la sociedad contemporánea, más allá de las relaciones cara a cara, se privilegia el contacto virtual resguardado mediante una identidad virtual, una especie de mascara virtual: cada persona tiene una huella o marca de su registro en el ciberespacio. Esto hace que las personas, en tanto que cibernautas tengan una primera forma de exposición hacia un "otro", el cual -como se expuso- puede configurarse en una eventual amenaza en tanto que "imagen idealizada sobre la cual se constituye la identidad personal" (como parece suceder con *Instagram* y las afectaciones a la salud mental), o bien, como "un otro enmascarado cuyas intenciones puedan ser "delictivas".

Para el caso particular de los niños, niñas y adolescentes, si bien tienden a mostrar más competencias digitales por el efecto de su exposición generacional, siguen siendo personas vulnerables a los riesgos existentes justamente por esta sobrestimación a sus capacidades, por exceso de confianza y falta de malicia ante lo que el entorno presenta. Adicionalmente, cuando

la comunicación está mediada puede, eventualmente, facilitar formas de interacción tendientes, en cierta medida a la despersonalización y a facilitar formas más fáciles para persuadir y engañar (mediante estrategias de ingeniería social) que pueden facilitar el acceso "al otro" y diluir las barreras de comunicación, convirtiéndose de tal manera, en un factor que activa la exposición a las amenazas existentes en el mundo virtual. Esto no quiere decir que, sin embargo, que exista un riesgo mayor en las interacciones que se dan en línea *versus* las que se dan en la realidad, pero las formas de control son más difíciles por el efecto de la viralización y la instantaneidad con la que se difunden los mensajes.

Como se vio anteriormente, el emprendimiento y desarrollo de acciones contra los delitos informáticos ha tenido que impulsarse más activamente por la emergencia, cada vez mayor, de acciones que atentan contra la seguridad de las personas, en tanto que cibernautas. Es palpable la necesidad del fortalecimiento de leyes en materia asociada con la protección de los niños, niñas y adolescentes, así como relacionadas con el resguardo de la identidad en casos de suplantación.

Como cibernautas, todos estamos expuestos al riesgo y podemos ser perceptores de amenazas, en ese sentido somos vulnerables; aunque esta posible inseguridad sea relativa a la persona, esto se potencia si el individuo no toma de medidas de precaución o prevención que lo exponga libremente a las amenazas existentes, tales como medidas de seguridad, o de protección de la información, precauciones en relación con la seguridad de la información que se comparte, esto hace que sea más fácil exponerse a un riesgo determinado. En este sentido, aunque no exista una vinculación con la Internet, hoy por hoy, siempre va a haber una vinculación con la tecnología, por ejemplo, solo con pertenecer a las bases públicas del Registro Civil o del Registro Nacional queda expuesto. De igual manera, se deben considerar los diferentes niveles de riesgo, pues puede haber un grado mayor de vulnerabilidad que está dada por existencia de una posible brecha digital, o por un desconocimiento eventual de los riesgos que podría tener una persona. De tal manera, a pesar de que ella no esté usando la red, podría ocurrirle una amenaza y ni siquiera estarse dando cuenta ni tomar medidas para estar revisando.

En términos generales, se puede afirmar que el riesgo cero no existe y que, en la medida de que somos usuarios de Internet, nos vemos expuestos a él, aunque se tomen medidas de seguridad o precaución siempre existe un riesgo residual de que algo pueda ocurrir. Retomando la perspectiva de Roberto Lemaître, si una persona no usa Internet o no tiene redes sociales, su riesgo puede ser menor, pero no es inexistente. Se podría decir que bajo ese escenario no le va a pasar nada, pero esto no es cierto, porque, aunque uno no quiera, hay información personal en bases de datos públicas, que podrían prestarse para eso [para exponerse a la amenaza]. Incluso adultos mayores que no tienen vinculación de las cuentas bancarias con la Internet han sido suplantados, les han abierto cuentas [se refiere a robo de información y suplantación de identidad], se han usado sus datos para cometer fraudes. (R. Lemaître, comunicación personal, 27 de noviembre de 2017).

Esto indica que la amenaza es latente y que siempre va a existir. Quiere decir entonces que los individuos, las empresas, las instituciones vienen a ser llamadas a controlar y tomar medidas de protección y de ciberseguridad. Esto plantea, por lo tanto, la necesaria articulación de acciones integrales, desde diferentes frentes y considerando a todas las poblaciones implicadas.

Desde la perspectiva de los individuos y las empresas

Las acciones recomendadas se encuentran en la prevención y vigilancia cotidianas. En el caso de las personas y las potenciales amenazas existentes como usuarios de servicios bancarios, por ejemplo, se indica que la prevención es la mejor ruta de acción para anticipar un riesgo y una amenaza; en este sentido debe imperar una actitud desconfiada y maliciosa. Si bien es cierto, hay una astucia y conocimiento -que es además apoyado- por estrategias como la ingeniería social- en los ciber-delincuentes, un comportamiento vigilante e intuitivo del individuo es la que debe activarse en tales casos. En la entrevista personal realizada al Señor Eric Lewis, él hacía la semejanza con respecto a la misma actitud que las personas deben tener hoy por hoy cuando transitan por las calles josefinas.

Se sugieren algunas acciones relevantes para considerar en todos momentos, tanto previsores como reactivos a los casos o situaciones de amenazas, tales como:

- Manejo de las reacciones personales: si la persona es víctima y si ya ha ocurrido un delito informático, la principal acción es recibir asesoría inmediata, esto con el fin de poder documentar la situación cuando se interpone una denuncia como forma de poder comprobar el evento y poder reconstruirlo. De acuerdo con Erik Lewis, muchas veces, desde la perspectiva de la investigación forense que se hace, registros de prueba como los pantallazos no son la forma idónea para poder dar seguimiento y valorar el perfil exacto desde el cual se está haciendo el acto delictivo.
- Identificar y recurrir a soluciones de seguridad construidas con tecnologías integradas.
- No responder ningún mensaje de correo electrónico sospechoso o de remitentes desconocidos.
- Nunca ingresar las contraseñas personales, sobre todo bancarias, a algún sitio al que se llegó por correo electrónico.
- Evitar proporcionar información financiera y llamar directamente a la institución bancaria ante cualquier duda.
- Siempre tener presente: ninguna entidad financiera, ni los operadores de tarjetas de crédito, solicitan datos personales a sus clientes o verificación de sus cuentas mediante correo electrónico, mensaje de texto o vía telefónica, a menos que el usuario haya sido quien contactó primero a la institución financiera.
- Cambiar constantemente las contraseñas. Además, es poco recomendable utilizar la misma contraseña para todo, y dedicar una sola, específicamente para los servicios de su banca, reduce la posibilidad de que roben información.

Desarrollo de programas y políticas para la educación y cultura digitales

La amenaza se puede potenciar o disminuir según el contexto de la persona, el cual integra también elementos asociados a la capacidad del individuo de discernir y valorar lo que puede ser eventualmente o no ser un peligro, esto remite a aspectos propios del desarrollo individual, al conocimiento y cultura digital, es decir al acervo de competencias que el individuo tenga o haya desarrollado sobre las tecnologías y el mundo digital. Esto indica que la ciberseguridad y la cultura digital son frentes de acción que deberían potencializarse desde la articulación de programas de formación temprana. En un mundo altamente especializado, ya es innegable que esto debe integrarse dentro de los planes y programas de educación formal, desde los primeros años de educación y continuando de forma constante en todo el proceso formador. Tanto como en los usos, dominios y competencias tecnológicas, estos programas deberán focalizarse también en formar actitudes conscientes acerca del potencial de Internet, como también de los riesgos que implica su uso, fomentando la prevención. Adicionalmente, resulta conveniente también crear y desarrollar consciencia acerca del poder formador, pero también destructor que puede tener Internet, las redes y las diferentes aplicaciones en la vida de las personas; si su uso no se acompaña del criterio, la capacidad de distinción y discernimiento frente al comportamiento en masa, la discriminación y balance en el uso excesivo, desmedido o descontrolado, e incluso en las intenciones que moderan este uso. La Internet es una herramienta de gran provecho si con ella todos aprendemos a formar actitudes, comportamientos y valores que lejos de asemejar los comportamientos agresivos y violentos que prevalecen en el mundo *offline*, promuevan una educación y cultura digitales hacia la paz y el bienestar personal.

Para el caso de la niñez y la adolescencia, es evidente que las acciones no pueden encontrarse en limitar el uso de la tecnología, en tanto es cada vez creciente en acceso y asequibilidad; las acciones deben centrarse más bien en enseñar a usar, lo cual está muy relacionado con la formación en ciberseguridad. Más que evitar la exposición de niños o jóvenes a ciertos contenidos, se debe hacer entender y comprender los riesgos de los comportamientos en Internet y cómo reaccionar ante contenidos dañinos o nocivos. La tecnología y todo su potencial no es necesariamente dañino, el problema deviene por las formas en que se usa y en cómo se usa, así como en las consecuencias que este mal uso tiene en las poblaciones. El problema más importante no es que todas las personas se encuentran expuestas a los riesgos y las amenazas, pues la diferencia sustancial en la afectación que esta última tiene viene dada por el uso que se da a las tecnologías y por la capacidad de saber utilizar las herramientas convenientemente.

Las poblaciones costarricenses, en general, deberían interesarse en conocer más y mejor las normativas existentes, tanto en términos de sus derechos como de los deberes que tienen como ciudadanos en estos temas que les atañe ya completamente

en todos los ámbitos de la vida cotidiana. Por ejemplo, si bien es cierto que la *Ley 8968*, de *Protección de la Persona contra el Tratamiento de sus Datos Personales* es relativamente "nueva" (en tanto tiene 6 años de estar en vigencia), las personas y organizaciones deberían ir avanzando en el cumplimiento de esta normativa e ir interiorizando cuáles son los derechos en esta materia específica. Esto reitera entonces la necesidad de una formación constante, regular e integrada dentro de la cultura. Pues, por ejemplo, si bien es cierto que muchos datos son de acceso público, esto no significa que las personas puedan hacer uso libre e indiscriminado de ellos, se debe dar un tratamiento adecuado que resguarde los derechos de cada una de las personas.

Como llamado a las acciones para convertir Internet en un espacio de navegación más seguro, principalmente para niños, niñas y adolescentes, se celebra, cada febrero, el Día de la Internet Segura (*Safer Internet Day),* esta es una iniciativa impulsada por la Unión Europea, que se desarrolla en 130 países y que también se lleva a cabo en Costa Rica (Vargas, 12 de febrero de 2018). Iniciativas como esta ayudan a concientizar sobre los derechos de los ciudadanos en relación con la protección de sus datos personales, pero también acerca de los cuidados y protecciones que deben tener en materia de ciberseguridad, pues muchos de los riesgos emergen por descuido o por falta de educación en temas relacionados con la seguridad informática y las herramientas que existen para tal fin. Al lado de estas propuestas, es también relevante reconocer la importancia de la actitud vigilante y cercana de los padres y madres, favoreciendo situaciones que promuevan la confianza para conversar sobre estos temas y favorecer el aprendizaje de posibles situaciones amenazantes o de riesgo y cómo manejarlas para evitarlas. Nuevamente, los espacios de diálogo, de reflexión y apertura son los favorecedores de actitudes preventivas.

Desde la perspectiva de empresas y organizaciones

Frente a la sofisticación y organización de las nuevas estrategias cada vez más articuladas para atentar contra la seguridad, diseñar respuestas tecnológicas de atención integral, que se renueven constantemente:

- Implementar soluciones que permitan operar la seguridad mediante automatización de las respuestas, la aplicación de la inteligencia artificial y el autoaprendizaje para que sean las redes las que adopten acciones de modo automático e inmediato.
- Verificar que las soluciones tecnológicas utilicen la inteligencia para procesar amenazas y entramados de seguridad que pueden configurarse de manera dinámica.
- Impulsar que la seguridad en las redes permita identificar, aislar y remediar rápidamente los dispositivos comprometidos o contaminados para contrarrestar los ataques.
- Integrar la "higiene de seguridad básica" a los protocolos de seguridad de las computadoras, sean personales, institucionales u organizacionales.
- Generar y aplicar correctamente protocolos de seguridad para el resguardo de la información. Los pilares fundamentales que deben estar vigentes para proteger la seguridad de la información son: la confidencialidad, la integridad y la disponibilidad. Esto permite valorar aspectos relacionados con una posible vulnerabilidad de sistemas, esto implica valorar aspectos relacionados con autenticaciones de usuarios, restricciones diarias de acceso y utilización de datos (muy relevante en las instituciones financieras y bancarias).

A modo de conclusión

Las consecuencias de lo que hemos presentado hasta este momento no son, de ninguna manera, un asunto eminentemente material. La cantidad de personas adultas, niños, adolescentes, jóvenes, pero sobre todo sujetos vulnerables que se han visto seriamente afectados, y que inclusive han optado por el suicido crece en todos los países. Los individuos no siempre están lo suficientemente informados, y no ha habido una cultura preventiva ni de desarrollo de competencias hacia la ciberseguridad. El desconocimiento, la ingenuidad y el exceso de confianza son parte de la vulnerabilidad existente; en el caso de los niños y los adolescentes, el panorama es algo más complejo en tanto implica repensar los límites de monitoreo, seguimiento o control; en otras palabras, no siempre podemos protegerlos porque no debemos invadir sus vidas ni su mundo privado, aunque éste se mueva en una esfera pública.

En vista de lo anterior, las estrategias que son efectivamente accionables se encuentran en el desarrollo de programas de

información y concientización en todos los niveles, tanto en los ámbitos de las políticas que permitan desarrollar leyes de vigilancia y control, como desde las instituciones públicas y privadas, los contextos escolares y colegiales y desde los escenarios parentales. Así, por ejemplo, aún sigue siendo un gran reto desarrollar estrategias de rehabilitación y tratamiento psicológico para personas que se han visto afectadas por situaciones de *bullying/ciberbullying* o *sexting*, sobre todo en las poblaciones más jóvenes. Desde otro nivel de injerencia, resulta pertinente desarrollar investigaciones más profundas que indaguen acerca de las mediaciones tecnológicas y sus consecuencias individuales, pero de ninguna manera esto se puede hacer disciplinariamente, debe implicar el conocimiento especializado de profesionales en informática, en seguridad, forenses, antropólogos, psicólogos y expertos ingenieros en *Big Data*.

Amaryllis Quirós-Ramírez

Investigadora en Prosic. Máster en Investigación en Psicología y Licenciada en Psicología de la Universidad de Costa Rica. Profesora de la Escuela de Psicología y del Postgrado en Psicología de esta misma Universidad. Investigadora en el área de las TIC y el desarrollo en el ciclo vital.

amaryllis.quiros@ucr.ac.cr

9.8 REFERENCIAS BIBLIOGRÁFICAS

Acurio Del Pino, S. (s.f.). *Delitos informáticos: Generalidades.* Recuperado de http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Álvarez, V., Rodríguez, A., & Cuevas, F. (2009). E-juventud en Costa Rica. En Prosic (Ed.), *Informe 2008: Hacia la sociedad de la información y el conocimiento*. San José, Costa Rica: Prosic, Universidad de Costa Rica.

Arcila, C. (2011). Análisis comparativo de la presentación personal virtual en diferentes espacios de interacción. *Fonseca, Journal of Communication, 3*, 154-169. Recuperado de http://revistas.usal.es/index.php/2172-9077/article/view/11907

Arcila, C. (2010). *La presentación del sí-mismo en los entornos virtuales: Comunicación, alteridad e identidad en chats, blogs y redes sociales* (Tesis doctoral). Recuperado de https://www.ucm.es/data/cont/media/www/pag-73273/TESIS%20ARCILA,Carlos(2010).pdf

Arcila, C. (s.f). La presentación de la persona en los entornos virtuales: El sí-mismo y el otro en la comunicación digital. *Razón y Palabra: Primera Revista Digital en Iberoamérica especializada en Comunicología*, *66.* Recuperado de http://www.razonypalabra.org.mx/N/n66/varia/carcila.html

Barnard-Wills, D., & Ashenden, D. (2012). Securing Virtual Space: Cyber War, Cyber Terror, and Risk. *Space and Culture*, *15*(2), 110-123. doi: 10.1177/1206331211430016.

Bonilla, I., & Vargas, E. (2012). *Estudio exploratorio del uso y riesgos de las redes sociales por parte de niños y niñas en edad escolar del Área Metropolitana: Caso de la Escuela Juan Rafael Mora Porras y de la Escuela Saint Jude* (Tesis de maestría). Universidad Estatal a Distancia. San José, Costa Rica.

Canto, J., & Moral, F. (2005). El sí mismo desde la teoría de la identidad social. *Escritos de Psicología, 7*, 59-70. Recuperado de http://www.redalyc.org/articulo.oa?id=271020873006

Celada, C. (2014). *El Cyberbullying como una nueva forma de delincuencia informática*. San José, Costa Rica: Publitex Grupo Editorial S.A.

Chacón, K. (20 de setiembre de 2015). Hackeo en CCSS enciende alarmas en seguridad de datos personales. *El Financiero*. Recuperado de https://www.elfinancierocr.com/tecnologia/hackeo-en-ccss-enciende-alarmas-en-seguridad-de-datos-personales/KVYT2VYBONGTNPMCQHMGHU3L5E/story/

Chacón, K. (17 de junio de 2016). *El Financiero.* https://www.elfinancierocr.com/tecnologia/casi-la-mitad-de-las-empresas-costarricenses-sufrieron-ataques informaticos/MF43YJFS5BHQLIVW32ML5T5A4M/story/

Chinchilla, D., Fallas, M. J., Rodríguez, F., & Sáenz, S. (2015). Victimización online en Costa Rica. *Encuesta Actualidades 2015*, Escuela de Estadística, Universidad de Costa Rica. Recuperado de http://www.estadistica.ucr.ac.cr/contenido/noticias/ESTADISTICA%20ENCUESTA%20ACTUALIDADES%202015.pdf

CISCO. (2016). *Annual Report 2016*. Recuperado de https://www.cisco.com/c/dam/en_us/about/annual-report/2016-annual-report-full.pdf

Código Penal de Costa Rica (s.f). Recuperado de http://www.oas.org/dil/esp/codigo_penal_costa_rica.pdf

Cordero, C. (20 de noviembre de 2017). Los 'hackers' también aplicarán la inteligencia artificial para atacar en 2018. *El Financiero.* Recuperado de http://www.elfinancierocr.com/tecnologia/los-hackers-tambien-aplicaran-la-inteligencia/5V25LLFCXNEWNGJOJ6HKHVVS54/story/

Erikson, E. (2009). *Infancia y sociedad*. Buenos Aires: Horme-Paidós.

Foucault, M. (2002). *Vigilar y castigar: Nacimiento de la prisión*. Buenos Aires: Siglo XXI.

Gercke, M. (2009). Enfoque jurídico para tipificar el delito de hurto de identidad. Documento de trabajo de la tercera reunión del grupo de expertos en delitos sobre identidad celebrada en Viena. Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC, 2013).

Goffman, E. (2001). *La presentación de la persona en la vida cotidiana.* Buenos Aires: Amorrortu Editores.

Grillo, M., Durán, J., & Esquivel, W. (2009). *Expresiones de violencia interpersonal y social en el ciberespacio desde la vivencia adolescente: Estado del arte de la investigación*. Recuperado de http://pep.ieepo.oaxaca.gob.mx/recursos/multimedia/DMAI_Clicseguro/archivos/Informe_Costa_Rica.pdf

Hootsuite. (2918). Reporte *Digital in 2018: Essential Insights into Internet, Social Media, Mobile and E-Commerce Use Around The World.* Recuperado de https://wearesocial.com/blog/2018/01/global-digital-report-2018

Lifebelt. (2016). Estudio de redes sociales en Centroamérica y el Caribe iLifebelt 2016. Recuperado de http://ilifebelt.com/6to-estudio-anual-ilifebelt-redes-sociales-centroamerica-caribe-2016/2016/08/

Latamclick. (2016). Estadísticas de Facebook y Twitter en Costa Rica 2016. Recuperado de https://www.latamclick.com/estadisticas-de-facebook-y-twitter-en-costa-rica/

Lemaître, R. (2012). Ciberseguridad en Costa Rica. En Prosic (Ed.), *Informe 2012: Hacia la Sociedad de la Información y el Conocimiento*, (pp. 309-338). San José, Costa Rica: Prosic, Universidad de Costa Rica.

Lenhart, A. (2009). *Teens and Sexting: How and Why Teens are Sending Sexually Suggestive Nude or Nearly Nude Images Via Text Messaging*. Recuperado de http://www.pewinternet.org/files/old-media/Files/Reports/2009/PIP_Teens_and_Sexting.pdf

Lenhart, A. (2010). *Teens, Adults and Sexting: Data on Sending/Receiving Sexually Suggestive Nude or Nearly Nude Photos by Americans.* Recuperado de http://www.pewinternet.org/2010/10/23/teens-adults-and-sexting-data-on-sendingreceiving-sexually-suggestive-nude-or-nearly-nude-photos-by-americans/

Lewis, E. (2010). Ingeniería social. En Programa Sociedad de la Información y el Conocimiento [Prosic], *Ciberseguridad en Costa Rica* (pp. 167-176). San José, Costa Rica: Prosic, Universidad de Costa Rica.

Liu, H. (2007). Social Network Profiles as Taste Performances. *Journal of Computer-Mediated Communication*, *13*(1). doi: 10.1111/j.1083-6101.2007.00395.x

Manago, A., Graham, M. B., Greenfield, P., & Salimkhan, G. (2008). Self Representation and Gender on MySpace. *Journal of Applied Developmental Psychology*, *29*(6), 446-458. doi: 10.1016/j.appdev.2008.07.001

Mead, G. H. (1968). *Mind, Self and Society.* Buenos Aires: Paidós.

Megías, I., & Rodríguez, E. (2014). *Jóvenes y comunicación: La impronta de lo virtual*. Recuperado de http://revistes.ub.edu/index.php/der/article/view/15405

Moore, T., & Clayton, R. (2007). *An Empirical Analysis of the Current State of Phishing Attack and Defence*. Computer Laboratory, University of Cambridge. Recuperado de https://www.cl.cam.ac.uk/~rnc1/weis07-phishing.pdf

Nagy, P., & Koles, B. (2014). The digital transformation of human identity: Towards a conceptual model of virtual identity in virtual worlds. *Convergence: The International Journal of Research into New Media Technologies*, 1-17. doi: 10.1177/1354856514531532.

Núñez, E., Villarroel, C., & Cuevas, V. (s.f). *Suplantación de la identidad.* Recuperado de www.gpd.sip.ucm.es/sonia/.../Suplantacion%20Identidad/Suplantacion_Personalidad.pdf

Oficina de las Naciones Unidas Contra la Droga y el Delito. (2013). Manual sobre delitos relacionados con la identidad. Recuperado de https://www.unodc.org/documents/organized-crime/13-83700_Ebook.pdf

Pantic, I. (2014). Online Social Networking and Mental Health. *Cyberpsychology, Behavior and Social Networking*, *17*(10), 652-657. Doi: 10.1089/cyber.2014.0070

Papacharissi, Z. (2002). The Presentation of Self in Virtual Life: Characteristics of Personal Home Pages. *Journalism and Mass Communication Quarterly, 79*(3), 643-660. Recuperado de http://www.etchouse.com/mcma503/readings.old/papacharissi-2002b.pdf

Pew Research Center. (2016). *New Use Accross Social Media: Platforms 2016*. Recuperado de http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/

Pérez Sánchez, R. (2013). Infancia, socialización y TIC. En Prosic (Ed.), *Informe 2013: Hacia la Sociedad de la Información y el Conocimiento*, (pp. 343-368). San José, Costa Rica: Prosic, Universidad de Costa Rica.

Pérez Sánchez, R. (2016). Adolescencia, socialización y TIC. En Prosic (Ed.), *Informe 2015: Hacia la Sociedad de la Información y el Conocimiento*, (pp. 99-118). San José, Costa Rica: Prosic, Universidad de Costa Rica.

Pérez, R., Rumoroso, A., & Brenes, C. (2009). El uso de tecnologías de la información y la comunicación y la evaluación de sí mismo en adolescentes costarricenses. *Interamerican Journal of Psychology, 43*(3), 610 – 617. Recuperado de http://pepsic.bvsalud.org/pdf/rip/v43n3/v43n3a21.pdf

Pettigrew, T. F. (1998). Intergroup Contact Theory. *Annual Review of Psychology*, *49*, 65-85.

Portillo, J. (2016). Planos de realidad, identidad virtual y discurso en las redes sociales. *Logos: Revista de Lingüística, Filosofía y Literatura*, *26*(1), 51-63. doi: 10.15443/RL2604.

Programa Sociedad de la Información y el Conocimiento [Prosic]. (2010). *Ciberseguridad en Costa Rica*. San José, Costa Rica: Prosic, Universidad de Costa Rica.

Proyecto de ley "Ley especial para la protección de los derechos de la niñez y la adolescencia frente a la violencia y el delito en el ámbito de las tecnologías de la información y la comunicación y reformas al Código Penal", expediente n 18.230, *La Gaceta* (2013). Recuperado de http://www.gaceta.go.cr/pub/2013/07/08/COMP_08_07_2013.pdf

Rodríguez, R. (2016). ¿Qué seguridad? Riesgos y amenazas de Internet en la seguridad humana. *Araucaria: Revista Iberoamericana de Filosofía, Política y Humanidades, 36*, 391-415. doi: 10.12795/araucaria.2016.i36.17

Royal Society for Public Health. (2017). *Instagram ranked worst for the Young peoples´s mental health.* Recuperado de https://www.rsph.org.uk/about-us/news/instagram-ranked-worst-for-young-people-s-mental-health.html

Salimkhan, G., Manago, A. M., & Greenfield, P. (2010). The Construction of Virtual Self on MySpace. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 4*(1). Recuperado de https://cyberpsychology.eu/article/view/4231/3275

Solano, J. (31 de enero de 2017). Aumentan denuncias por extorsión sexual vía Internet. *crhoy.com*. Recuperado de https://www.crhoy.com/nacionales/aumentan-denuncias-por-extorsion-sexual-via-internet/

Turner, J. C. & Reynolds, K. (2003). The Social Identity Perspective in Intergroup Relations: Theories, Themes, and Controversies. En R. Brown, & S.L. Gaertner (Eds.), *Blackwell Handbook of Social Psychology: Intergroup Processes*, (pp.133-152). United Kingdom: Blackwell Publising.

Varela, I. (15 de marzo de 2017). Colegiales de 7º a 9º son más propensos al "ciberbullying". *La Nación*, p. 14A.

Vargas, M. (12 de febrero de 2018). Aprenda a hacer de Internet un espacio más confiable. *La Nación*, p. 14A.

Entrevistas

Erik Lewis, Jefe de la Sección de Delitos Informáticos del *Organismo de Investigación Judicial (OIJ).* 18 de setiembre de 2017.

Roberto Lemaître Picado, abogado-ingeniero informático, especialista en delitos informáticos; Profesor de la Universidad de Costa Rica. 27 de noviembre de 2017.